RISE OF DIGITAL CONSTITUTIONALISM

Padala Tharun Prabhakar, Damodaram Sanjivaya National Law University, Visakhapatnam

ABSTRACT

The rapid expansion of digital technology has significantly transformed communication, governance, democratic participation, and the exercise of constitutional rights. In response to these developments, the concept of digital constitutionalism has emerged to ensure that constitutional values such as freedom of speech, privacy, equality, transparency, and accountability extend into digital environments. This article examines the evolution and significance of digital constitutionalism with particular reference to Indian constitutional jurisprudence. It analyses landmark judicial decisions, including Shreya Singhal v. Union of India, Justice K.S. Puttaswamy v. Union of India, Anuradha Bhasin v. Union of India, Faheema Shirin R.K. v. State of Kerala, and Amar Jain v. Union of India, which collectively demonstrate the judiciary's attempt to adapt constitutional protections to digital realities. The article further discusses contemporary concerns regarding surveillance, intermediary liability, algorithmic discrimination, and data governance through developments such as the Pegasus spyware controversy, the DPDP Act, X Corp v. Union of India, and the Dutch Childcare Benefits Scandal. The article concludes that digital constitutionalism is essential for ensuring that technological advancement remains compatible with democratic governance, human dignity, and fundamental rights in the digital age.

1. Introduction

The growth of digital technology has fundamentally changed the manner in which individuals communicate, participate in democratic processes, and exercise constitutional freedoms. Social media platforms, virtual communities, online marketplaces, and artificial intelligence systems now influence everyday life on an unprecedented scale. Activities such as political discussion, public protest, education, employment, and economic participation increasingly occur within virtual spaces rather than traditional physical environments.

Traditional constitutional law was developed in an era where governance was closely connected to territorial boundaries and physical institutions. Constitutional protections were primarily designed to regulate State action within geographical territory. However, the rise of digital technology has created new forms of governance and power that frequently operate beyond territorial limitations. Private technology companies now regulate speech, collect personal data, influence public discourse, and shape democratic participation through digital platforms.

This transformation raises an important concept called Digital Constitutionalism. The increasing dependence upon digital environments demonstrates that constitutional law can no longer remain confined solely to physical public spaces. As democratic participation increasingly shifts online, constitutional systems must adapt to ensure protection of liberty, privacy, equality, and freedom of expression in virtual environments.

2. Rise of Digital Constitutionalism

Digital constitutionalism refers to the application of constitutional values and democratic principles within digital environments. It seeks to protect fundamental rights in cyberspace and regulate digital power exercised by both governments and private technology companies.

The concept emerged in response to the growing influence of digital platforms over communication, political participation, and social interaction. As technology companies acquired greater control over online speech and personal data, scholars and courts increasingly recognised the need for constitutional protections in virtual spaces.

Digital constitutionalism is founded upon several fundamental principles that seek to preserve constitutional values within the rapidly evolving digital environment. Let us discuss the core

aspects of Digital Constitutionalism.

2.1 Freedom of speech and expression

In the digital age, the internet and social media platforms have become major spaces for public discourse, political participation, and the exchange of ideas. Digital constitutionalism emphasizes that individuals must enjoy the same freedom of expression online as they do offline, subject to reasonable restrictions necessary for public order, security, and morality. It aims to prevent arbitrary censorship, unlawful content restrictions, and excessive governmental or corporate control over online communication. In the Indian context, this principle received strong constitutional recognition in Shreya Singhal v. Union of India,[1] where the Supreme Court of India struck down Section 66A of the Information Technology Act, 2000, on the ground that it violated the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution. The Court observed that vague and overbroad expressions such as "offensive" or "annoying" in Section 66A could lead to arbitrary arrests and suppression of legitimate online expression. This landmark judgment became a foundational development in India's digital constitutional framework, as it reaffirmed that constitutional protections extend equally to speech in digital spaces and that state regulation of online communication must satisfy constitutional standards of reasonableness and legality.

X Corp v. Union of India[2] is another important contemporary case dealing with the relationship between digital governance, intermediary liability, free speech, and state censorship in India. The case was filed by X Corp before the Karnataka High Court challenging the Government of India's use of the "Sahyog Portal" for directing online content takedowns.

The central issue in the case is whether the government can use Section 79(3)(b) of the Information Technology Act, 2000, to compel intermediaries such as X to remove online content, or whether such blocking orders can only be issued under Section 69A of the IT Act, which contains procedural safeguards. X Corp argued that Section 79 merely provides conditional "safe harbor" protection to intermediaries and does not independently authorize censorship or blocking orders. According to X, only Section 69A permits the government to block content, and even then, such action must follow due process, written reasons, and

[1] AIR 2015 SC 1523
[2] WP 7405/2025

procedural safeguards recognized by the Supreme Court in Shreya Singhal v. Union of India.

The dispute mainly arose because of the government's "Sahyog Portal," created by the Ministry of Home Affairs through the Indian Cyber Crime Coordination Centre (I4C). The portal allows government agencies to request intermediaries to remove allegedly unlawful content. X Corp contended that the portal effectively creates an indirect censorship mechanism because failure to comply may expose intermediaries to liability for third-party content. The company also argued that many takedown requests targeted political criticism, opposition voices, and dissenting opinions, thereby affecting the constitutional right to freedom of speech and expression under Article 19(1)(a).

On the other hand, the Union Government argued that safe harbor protection under Section 79 is conditional and intermediaries operating in India must comply with Indian laws and due diligence obligations under the IT Rules, 2021. The government maintained that national security, sovereignty, and public order justify such regulatory measures.

From a constitutional perspective, the case raises a major question about balancing free speech with national security in the digital age. Critics argue that vague expressions such as "threat to sovereignty" or "public order" may be interpreted broadly, leading to excessive censorship and suppression of legitimate political criticism. Therefore, the case has become highly significant for digital constitutionalism because it concerns transparency, accountability, intermediary autonomy, and constitutional limitations on digital censorship by the State.

The matter is currently pending before the Karnataka High Court, and its final outcome may substantially influence the future of online free speech regulation and platform governance in India.

2.2 Right to privacy

Another significant principle of digital constitutionalism is the protection of privacy and informational autonomy. With the rapid growth of digital technologies, governments and private corporations collect vast amounts of personal data through online activities, surveillance systems, artificial intelligence, biometric technologies, and digital platforms. Digital constitutionalism seeks to safeguard individuals from misuse of their personal information by recognizing privacy as a fundamental constitutional value. It promotes the right

of individuals to control their personal data, make informed choices regarding data sharing, and protect themselves against unauthorized surveillance, profiling, and data exploitation. Informational autonomy also ensures that individuals retain the freedom to shape their digital identity without coercion, manipulation, or intrusive state interference. In the Indian constitutional context, this principle was significantly strengthened in Justice K.S. Puttaswamy v. Union of India,[3] where the Supreme Court of India unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The Court acknowledged that in the digital era, unrestricted state surveillance, data collection, and technological monitoring pose serious threats to individual liberty, dignity, and autonomy. The judgment emphasized that privacy includes informational privacy and the protection of personal data from arbitrary intrusion by both the State and private entities. This landmark decision laid the constitutional foundation for data protection, digital rights, and limitations on mass surveillance in India, thereby becoming one of the most important judicial contributions to the development of digital constitutionalism.

The importance of privacy, transparency, and accountability in digital governance was further highlighted in Manohar Lal Sharma v. Union of India,[4] popularly known as the Pegasus spyware case. In this matter, allegations emerged that the Pegasus spyware, developed for covert surveillance, had been used to infiltrate the mobile devices of journalists, activists, lawyers, politicians, and other citizens without lawful authorization. The Supreme Court of India observed that there existed prima facie concerns regarding violations of digital privacy and constitutional freedoms through unauthorized surveillance. The Court emphasized that national security cannot be used as a blanket justification to avoid judicial scrutiny when fundamental rights are at stake. Consequently, it appointed an independent expert committee to investigate the allegations, reflecting the constitutional necessity of transparency and accountability in the exercise of state surveillance powers. The Pegasus case became a significant example of digital constitutionalism in practice, as it demonstrated judicial efforts to balance national security interests with individual privacy, civil liberties, and democratic accountability in the digital age.

2.3 Transparency and Accountability

Transparency in digital governance is another core aspect of digital constitutionalism. Modern

[3] (2017) 10 SCC 1
[4] AIR 2021 SC 5396

governance increasingly relies upon algorithms, automated decision-making systems, and digital platforms to deliver public services and regulate online activities. Digital constitutionalism demands that such systems operate transparently so that citizens can understand how decisions affecting their rights and freedoms are made. It encourages openness in governmental digital policies, platform regulations, and algorithmic processes to avoid secrecy, discrimination, and abuse of power. Transparent governance strengthens public trust and promotes democratic accountability in the digital sphere.

Closely connected with transparency is the principle of accountability of technological power. Large technology companies, digital platforms, and state authorities now exercise immense influence over communication, information flow, economic opportunities, and political discourse. Digital constitutionalism seeks to ensure that these powerful entities remain accountable for their actions and decisions. It advocates for legal mechanisms that regulate monopolistic behavior, prevent misuse of artificial intelligence, ensure responsible content moderation, and provide remedies for violations of digital rights. Accountability ensures that technological advancement does not undermine constitutional freedoms and democratic institutions.

The Digital Personal Data Protection Act, 2023 has generated serious constitutional concerns because many scholars, journalists, RTI activists, and civil society organisations argue that it weakens the transparency framework established under the Right to Information Act, 2005. The RTI Act has long been regarded as one of the strongest democratic tools for ensuring governmental transparency, exposing corruption, and promoting public accountability. However, critics contend that the DPDP Act, particularly Section 44(3), substantially dilutes these objectives by amending Section 8(1)(j) of the RTI Act.

Before the amendment, Section 8(1)(j) of the RTI Act allowed authorities to deny disclosure of personal information only when such disclosure had no relationship to public activity or would amount to an unwarranted invasion of privacy. Importantly, the earlier provision contained a "public interest override," which empowered Public Information Officers to disclose even personal information if a larger public interest justified disclosure. This safeguard was crucial because it enabled journalists, researchers, and citizens to seek information regarding corruption, misuse of public office, asset declarations, recruitment irregularities, public expenditure, and abuse of power by public officials.

The DPDP Act altered this balance by replacing the earlier nuanced provision with a broader exemption for "personal information." Critics argue that this change effectively creates a blanket shield against disclosure because almost any information connected to a public official can now be classified as personal data. The removal of the "larger public interest" exception means that authorities are no longer required to balance privacy against transparency. As a result, information that could reveal corruption or administrative wrongdoing may now be denied solely on the ground that it contains personal information.[5]

This development is seen as particularly dangerous because the RTI Act functions as a constitutional instrument of democratic accountability. In the writ petition filed in Supreme Court, The Reporters Collective Trust & Anr. v. Union of India & Ors.,[6] RTI activists argue that transparency is essential for enforcing constitutional values such as participatory democracy, responsible governance, and freedom of speech and expression under Article 19(1)(a). Investigative journalism and anti-corruption inquiries frequently rely on official records that contain personal details of public officials, including property disclosures, file notings, disciplinary proceedings, travel expenses, and procurement records. If all such information is treated as exempt personal data, the State may become insulated from public scrutiny.

Another major concern is that the DPDP Act creates an imbalance between citizens and the State. While the government receives broad powers to collect, process, and retain citizens' personal data under various exemptions and surveillance-related provisions, citizens are simultaneously denied access to governmental information on privacy grounds. Critics describe this as a paradox where the State gains greater informational power while public oversight mechanisms are weakened.

The constitutional challenge currently pending before the Supreme Court of India therefore argues that Section 44(3) of the DPDP Act is manifestly arbitrary and unconstitutional because it undermines the RTI Act's core purpose of transparency and accountability. Petitioners including RTI activists, journalists, and civil society groups contend that the amendment transforms the RTI framework from a "Right to Information" into a potential "Right to Deny

[5] https://internetfreedom.in/supreme-court-issues-notice-on-constitutional-challenge-to-the-digitalpersonal-data-protection-act-2023-and-the-digital-personal-data-protection-rules-2025/
[6] W.P.(C) No. 211/2026

Information."

Thus, although the DPDP Act was enacted to strengthen privacy and data protection following Justice K.S. Puttaswamy v. Union of India, critics argue that the law goes beyond protecting privacy and risks weakening democratic transparency. The debate ultimately reflects a larger constitutional conflict between two equally important democratic values: the right to privacy and the citizens' right to know.

2.4 Democratic Participation

Digital constitutionalism also promotes democratic participation in cyberspace. The digital environment has transformed the way citizens engage in democratic processes through online discussions, digital campaigns, electronic governance, and access to information. It seeks to create an inclusive digital public sphere where individuals can freely participate in civic activities and contribute to democratic decision-making. In recent years, digital platforms have demonstrated their growing influence not only in shaping public opinion but also in directly affecting political developments and leadership transitions. A significant example emerged in September 2025 in Nepal, where intense Gen Z-led anti-corruption protests and widespread public dissatisfaction with governmental corruption resulted in political instability and the collapse of the existing government. Following the imposition of a social media ban, activists and citizens increasingly turned to alternative digital communication platforms such as Discord to organize protests and coordinate civic participation. In a historic development, members of the "Youth Against Corruption" Discord server conducted an online voting process through which Sushila Karki was selected as the nation's first female interim prime minister.[7] This event illustrated how digital platforms can evolve into spaces of democratic engagement capable of influencing political leadership and constitutional governance. At the same time, such developments also highlight important constitutional concerns regarding legitimacy, transparency, digital security, and the regulation of online political mobilization. Digital constitutionalism therefore seeks to balance the democratic potential of cyberspace with safeguards against misinformation, digital manipulation, cyber interference, and unlawful concentration of technological power. By protecting digital civic spaces and ensuring fair participation in online democratic processes, digital constitutionalism strengthens

[7] https://www.realinstitutoelcano.org/en/analyses/nepal-elects-its-first-female-prime-minister-on-discord-wh at-it-reveals-about-social-media-and-democracy/

constitutional democracy in the modern digital age.

2.5 Equality and non-discrimination

Equality and non-discrimination constitute essential principles of digital constitutionalism in the contemporary digital age. As governance, banking, education, healthcare, employment, and welfare delivery increasingly shift to digital platforms, access to digital infrastructure has become necessary for meaningful participation in society. However, unequal access to technology and inaccessible digital systems often disproportionately affect marginalized communities, including persons with disabilities, economically weaker sections, rural populations, elderly citizens, women, students, and technologically disadvantaged groups. Digital constitutionalism therefore seeks to ensure that technological advancement does not reinforce existing social and economic inequalities but instead promotes inclusiveness, accessibility, and equal participation in digital environments.

The constitutional principle of equality under Article 14 requires that digital governance mechanisms remain fair, inclusive, and non-discriminatory. Mandatory digital procedures without accessible alternatives may exclude vulnerable individuals from accessing essential services and constitutional entitlements. This concern received significant judicial recognition in Amar Jain v. Union of India,[8] where the Supreme Court of India recognized the "right to digital access" as an integral part of the right to life under Article 21 of the Constitution. The case arose from a petition[9] filed by an acid attack survivor who was unable to complete mandatory e-KYC verification because facial recognition technology failed to accommodate facial disfigurement. The Court observed that inaccessible digital systems can result in indirect discrimination and exclusion from essential services, thereby violating constitutional guarantees of equality, dignity, and personal liberty. It further emphasized that the State has a constitutional obligation to create inclusive and accessible digital ecosystems that accommodate the needs of all citizens, particularly vulnerable and marginalized groups.

The principle that digital access forms an essential component of constitutional rights had also been recognized earlier in Faheema Shirin R.K. v. State of Kerala,[10] where the Kerala High Court held that access to the internet constitutes a part of the right to education and the right

[8] 2025 INSC 599
[9] Pragya Prasun v. Union of India, W.P.(C) No. 289 of 2024
[10] AIR 2020 Ker 35

to privacy under Article 21 of the Constitution. The Court invalidated restrictions imposed on students' internet usage in hostels and observed that access to the internet had become essential for acquiring knowledge, accessing educational resources, and participating in modern academic life. The judgment highlighted that unreasonable restrictions on internet access could disproportionately affect students and impede educational equality in an increasingly digital learning environment.

The reasoning adopted in Amar Jain and Faheema Shirin also reflects and extends the constitutional principles recognized earlier in Anuradha Bhasin v. Union of India,[11] where the Supreme Court acknowledged the constitutional importance of internet access for the exercise of freedom of speech and professional freedoms under Articles 19(1)(a) and 19(1)(g). While Anuradha Bhasin focused on protecting citizens against arbitrary restrictions on internet access, Faheema Shirin emphasized the relationship between internet access, education, and privacy, and Amar Jain further expanded this constitutional understanding by stressing that meaningful digital access must also remain inclusive, accessible, and non-discriminatory. Together, these judgments demonstrate the judiciary's evolving approach toward digital constitutionalism by recognizing that constitutional rights must remain effective and enforceable within an increasingly technology-driven society.

The Dutch Childcare Benefits Scandal represents one of the most significant global examples of algorithmic discrimination and its impact on constitutional values such as equality, non-discrimination, transparency, and accountability in the digital age. The scandal emerged when Dutch tax authorities used an automated risk-classification algorithm to detect alleged fraud in applications for childcare benefits. The algorithm relied upon factors such as nationality and ethnicity while generating "risk profiles," resulting in individuals of non-Dutch nationality and immigrant backgrounds being disproportionately identified as potential fraudsters. Amnesty International, in its report Xenophobic Machines, described the system as an example of racial profiling embedded within automated decision-making processes.[12] Tens of thousands of families, particularly from low-income and ethnic minority communities, were falsely accused of fraud, leading to severe financial hardship, debt, social stigma, and loss of livelihoods.

The scandal demonstrates the dangers posed by unregulated algorithmic governance and

[11] AIR 2020 SC 1308
[12] https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/

highlights how digital technologies may reproduce and intensify existing social prejudices when constitutional safeguards are absent. The use of nationality as a risk indicator reflected discriminatory assumptions that certain ethnic or migrant groups were more likely to commit fraud. As a result, the automated system violated principles of equality and non-discrimination by subjecting vulnerable communities to disproportionate scrutiny and punishment. The controversy ultimately became so serious that it contributed to the resignation of the Dutch government in 2021, illustrating the profound constitutional and political consequences of opaque technological governance.

From the perspective of digital constitutionalism, the Dutch scandal highlights the urgent need for transparency, accountability, and human rights protections in the deployment of artificial intelligence and automated decision-making systems. Amnesty International emphasized that governments increasingly rely on algorithms to deliver public services and detect fraud, yet the absence of adequate regulation and oversight can lead to systemic discrimination and violations of fundamental rights. The case therefore demonstrates that algorithmic systems used by the State cannot remain "black box" technologies immune from public scrutiny or constitutional review.

The scandal also has broader implications for digital governance worldwide, including in India, where governments are increasingly adopting AI-driven systems for welfare delivery, surveillance, digital identification, and administrative decision-making. It serves as a cautionary example that technological efficiency cannot override constitutional guarantees of equality, dignity, due process, and accountability. Digital constitutionalism therefore requires that algorithmic governance mechanisms remain transparent, explainable, non-discriminatory, and subject to judicial and democratic oversight to prevent digital technologies from becoming instruments of exclusion and systemic injustice.

3. Conclusion

Digital constitutionalism has emerged as one of the most significant constitutional developments of the twenty-first century. The rapid expansion of digital technologies, artificial intelligence, social media platforms, algorithmic governance, and data-driven administration has fundamentally transformed the relationship between the State, private technology companies, and citizens. In this evolving digital environment, traditional constitutional principles can no longer remain confined to physical spaces and territorial governance.

Constitutional protections relating to liberty, privacy, equality, freedom of speech, transparency, and democratic participation must now extend into cyberspace and digital ecosystems.

The judicial developments discussed in this article demonstrate the growing recognition that digital spaces have become integral to the exercise of fundamental rights. Decisions such as Shreya Singhal v. Union of India, Justice K.S. Puttaswamy v. Union of India, Anuradha Bhasin v. Union of India, Faheema Shirin R.K. v. State of Kerala, and Amar Jain v. Union of India collectively reflect the judiciary's attempt to adapt constitutional jurisprudence to technological realities. These cases recognize that internet access, informational privacy, digital participation, and inclusive technological systems are no longer optional conveniences but essential conditions for the meaningful enjoyment of constitutional freedoms and democratic citizenship.

At the same time, contemporary developments also reveal the dangers posed by unchecked digital power. The Pegasus spyware controversy, the constitutional concerns surrounding the DPDP Act and RTI framework, the ongoing dispute in X Corp v. Union of India, and the Dutch Childcare Benefits Scandal collectively demonstrate how surveillance technologies, opaque algorithms, platform regulation, and automated decision-making systems may threaten constitutional values when adequate safeguards are absent. These developments highlight that digital technologies are not politically neutral tools; rather, they possess the capacity to shape democratic participation, regulate public discourse, reinforce social inequalities, and concentrate unprecedented power in the hands of both States and private corporations.

Digital constitutionalism therefore represents an evolving constitutional response aimed at ensuring that technological advancement remains compatible with democratic governance and the rule of law. It seeks to establish constitutional limitations upon digital power while simultaneously protecting citizens from censorship, surveillance, algorithmic discrimination, exclusion, and misuse of personal data. The future of constitutional democracy increasingly depends upon the ability of legal systems to balance innovation with accountability and technological efficiency with human dignity.

Ultimately, digital constitutionalism reflects the broader constitutional principle that technological progress cannot be permitted to undermine fundamental rights. Instead, constitutional governance must evolve to ensure that digital transformation strengthens

democratic participation, transparency, inclusiveness, and human freedom in an increasingly interconnected digital society.

References

1. *Amar Jain v. Union of India* 2025 INSC 599.
2. *Anuradha Bhasin v. Union of India* AIR 2020 SC 1308
3. *Faheema Shirin R.K. v. State of Kerala* AIR 2020 Ker 35.
4. *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
5. *Manohar Lal Sharma v. Union of India* AIR 2021 SC 5396.
6. *Pragya Prasun v. Union of India* W.P.(C) No. 289 of 2024.
7. *Shreya Singhal v. Union of India* AIR 2015 SC 1523.
8. *The Reporters Collective Trust & Anr. v. Union of India & Ors.* W.P.(C) No. 211/2026.
9. *X Corp v. Union of India* WP 7405/2025.
10. https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-chil d-benefit-scandal/
11. https://internetfreedom.in/supreme-court-issues-notice-on-constitutional-challeng e-to-the-digital-personal-data-protection-act-2023-and-the-digital-personal-data-p rotection-rules-2025/
12. https://vidhilegalpolicy.in/blog/digital-access-as-a-fundamental-right/
13. https://ohrh.law.ox.ac.uk/right-to-education-emergence-of-a-digital-divide-in-digit al-india/