DIGITAL CONSTITUTIONALISM AND THE CHALLENGE TO CONSTITUTIONAL VALUES IN THE DIGITAL ERA

Aditya Singh & Shiv Bhushan Singh, St. Aloysius Institute of Technology and National Law University, Odisha

ABSTRACT

Digital technologies have created a complete transformation of power structures which now present new constitutional issues that existing legal systems cannot address. Traditional constitutional arrangements were built to constrain visible exercises of state authority through legal text, institutional checks, and judicial enforcement. The digital era, by contrast, utilizes hidden control methods which use data collection and algorithmic processing together with infrastructural design choices to control human behavior without needing laws or court approval. The constitutional focus of this matter requires a doctrinal solution which needs to move past judicial reactions toward active engagement with the basic elements of digital governance.

Digital constitutionalism functions as the framework which enables the confirmation of constitutional values in digital spaces. This research investigates how privacy rights and data protection laws and digital rights management systems create constitutional challenges which particularly affect the Indian constitutional framework. The article maintains that constitutional protections need to be redefined because they must restrict both government officials and private technological systems which function as governing technologies that produce governmental effects similar to legislative frameworks. The Digital Personal Data Protection Act 2023 and the Supreme Court decision in Justice K.S. Puttaswamy (Retd.) v. Union of India and the current court proceedings about the Aadhaar biometric identification system demonstrate how constitutional law must deal with digital power issues. The developments show how constitutional law develops through specific data-driven systems which dominate modern societies.

Keywords: Digital Constitutionalism, Right to Privacy, Data Protection and Surveillance, Digital Governance, Digital Rights Management (DRM), Indian Constitutional Law.

I. INTRODUCTION

The evolution of constitutional thinking developed through a specific power understanding which viewed state authority as held by specific government officials. The constitutional systems which restrict power through judicial rights and power division and procedural protection mechanisms were designed to regulate that particular power. The complete understanding of governance has changed because digital governance systems now operate in their current form. Power now uses hidden systems which include data transmission networks and automated decision-making systems and technological frameworks that control how people engage in social and public activities. The current constitutional debate centers on whether digital systems which now execute sovereign duties should receive the same legal protection that liberal democracies use to limit government authority.[1]

Digital platforms now function as the primary conduits through which citizens access information, engage in public discourse, and interact with state institutions. The platforms operate through their algorithms which filter content, generate revenue from user data, and implement user conduct standards through their technical framework thereby violating constitutional rights of freedom and equality and freedom of expression. The complete transfer of constitutional rights protection from government authority to digital platforms and from legal systems to software programming constitutes the main obstacle which has led to the emergence of digital constitutionalism as a research area and advocacy field.[2]

The ongoing development of state-operated digital systems which require biometric identification and use data for welfare distribution and employ algorithms for law enforcement purposes has created greater constitutional challenges which arise from state control over citizen privacy rights and freedom rights. The digital age brings new challenges to constitutional law because it multiplies existing governmental constitutional issues through technological means while also creating new constitutional problems which emerge from private entities that act with governmental authority.[3]

---

[1] Dennis Redeker, Lex Gill & Urs Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 80 Int'l Commc'n Gazette 302, 303 (2018).
[2] Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, 33 Int'l Rev. L. Computers & Tech. 76, 78 (2019).
[3] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 7-10 (PublicAffairs 2019).

The article contains four main chapters which develop its content. Chapter I evaluates how digital constitutionalism functions in the current constitutional governance system while assessing how digital technologies have changed power distribution and existing constitutional frameworks. Chapter II investigates privacy and data security because these areas show how constitutional rights face their most important challenges. Chapter III investigates digital rights management because it allows private organizations to control public affairs through their non-legal powers which escape constitutional control. The fourth chapter studies digital governance through constitutional doctrine in India to find the existing challenges for digital governance and its remaining gaps. The article demonstrates that digital constitutionalism needs to operate as a standard system which limits both governmental and private control of digital assets to protect fundamental constitutional principles.

II. DIGITAL CONSTITUTIONALISM AND THE TRANSFORMATION OF CONSTITUTIONAL GOVERNANCE

The analog period of constitutional governance depended on certain power assumptions which people considered obvious because they matched actual social behavior. Authority existed mainly as a public presence. The authority of power could be observed during specific times when officials granted their permission to execute their responsibilities. Government actions toward specific individuals had to meet constitutional standards of due process and equal protection and fundamental rights to achieve proper enforcement of these rights. The constitutional subject existed as a legal entity who engaged with a government system that functioned from a specific area through its established command hierarchy.

The digital transformation has dissolved each of these assumptions. Power in the digital era is distributed across state agencies, private corporations, and algorithmic systems that interact in ways that blur the public-private boundary and make any single act difficult to isolate as the proximate cause of a constitutional harm. As Dennis Redeker, Lex Gill, and Urs Gasser observed in their foundational account of digital constitutionalism, the emergence of the Internet created a new governance environment in which initiatives seeking to articulate rights, governance norms, and limitations on the exercise of power became necessary precisely because existing constitutional frameworks were insufficient to address the dispersed authority of digital systems.[4]

The term "digital constitutionalism" captures this movement to project constitutional values into digital governance structures. In its most rigorous formulation, offered by Edoardo Celeste,

[4]Redeker, Gill & Gasser, supra note 1, at 305-06.

digital constitutionalism is the ideology that adapts the values of contemporary constitutionalism to the digital society, functioning not merely as a collection of documents or declarations but as the normative orientation that informs the entire range of responses to the constitutional challenges of digital technology.[5] This definition has the advantage of distinguishing digital constitutionalism as a normative project from any particular institutional expression it might take, whether legislative, judicial, or regulatory.

Among the most significant structural features of digital governance that constitutional doctrine must address is the normalization of continuous surveillance as an ordinary administrative technique. Shoshana Zuboff has demonstrated in meticulous empirical and theoretical detail that the dominant business model of the digital economy, what she terms "surveillance capitalism," depends on the unilateral extraction of personal behavioral data from individuals who have no meaningful awareness of the scope of data collection or the purposes to which it is put.[6] Constitutional doctrines premised on the disclosure of the content and scope of state action before the fact, including the right to notice and the requirement of prior authorization for intrusions on liberty, do not readily accommodate a surveillance architecture that is pervasive, automatic, and largely invisible.

Lawrence Lessig introduced the foundational insight, now widely accepted in constitutional and legal theory, that code functions as law in digital environments.[7] Technical architectures regulate conduct as effectively as legal commands, but without the procedural constraints, democratic authorization, or judicial oversight that constitutional law imposes on formal exercises of governmental power. When an algorithm determines which citizens receive welfare benefits or flags individuals for further investigation by law enforcement, that determination has the practical force of a governmental decree. Constitutional doctrine that is confined to reviewing formal legal enactments will systematically fail to reach the increasingly important class of governance decisions that are implemented through technical design rather than legislative text.

The Indian Supreme Court's unanimous recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marks the most significant constitutional response in India to the challenges of digital governance. Justice Chandrachud, writing for himself and

[5]Celeste, supra note 2, at 80-81.
[6]Zuboff, supra note 3, at 63-66.
[7]Lessig, supra note 4, at 120-24.

three other judges, reasoned that privacy is not a gift of the state but an attribute of personhood that inheres in the individual by virtue of being human, and that in a digital society, the right to privacy encompasses informational autonomy: the power of individuals to control the terms on which personal information about them is collected, stored, and used.[8] This reasoning extends constitutional protection beyond physical spaces to the informational domain, recognizing that in an era of pervasive data collection, the ability to control one's personal information is inseparable from the freedom to form one's own beliefs and make authentic choices about how to live.

Yet the constitutional significance of *Puttaswamy* lies not only in its doctrinal content but in its structural implications. By grounding the right to privacy in human dignity and autonomy rather than in the specific catalogue of enumerated rights, the judgment creates a constitutional mandate for ongoing judicial engagement with the conditions under which digital systems affect the capacity of individuals to exercise self-determination. This mandate extends, in principle, to both state and non-state actors, though the doctrine of horizontal application remains contested and incompletely developed. Digital constitutionalism, as a normative framework, demands that this extension be made explicitly and operationalized through regulatory structures capable of reaching private actors.[9]

III. PRIVACY, DATA SECURITY, AND CONSTITUTIONAL VALUES IN THE DIGITAL ERA

Privacy has historically occupied an ambivalent position in Indian constitutional law. Prior to *Puttaswamy*, the existence of an independent constitutional right to privacy was doubtful, with earlier Supreme Court decisions in *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh* having held that the Constitution did not specifically protect privacy. The nine-judge bench in *Puttaswamy* overruled these decisions decisively, holding that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.[10] The judgment's constitutional significance extends beyond its doctrinal holding to the reasoning it advanced: privacy is understood as the condition that makes all other freedoms meaningful, the zone

[8]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 117 (Chandrachud, J.).
[9]Redeker, Gill & Gasser, supra note 1, at 312-13.
[10]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 3, 38 (Chandrachud, J.).

within which individuals can exercise genuine autonomy and form authentic identities.

The constitutional dimensions of digital era privacy protections extend beyond safeguarding physical access to private spaces. The continuous creation of personal data through digital activities in modern society has transformed privacy into a concept that differs from its understanding before the digital age. The right to informational self-determination gives individuals power over their personal data collection and usage and distribution rights. Puttaswamy recognized this transformation because Justice Chandrachud explained that digital technology created new privacy risks which needed constitutional protection.[11]

The primary legal framework which implements the constitutional right to informational privacy operates through data protection laws. The Digital Personal Data Protection Act of 2023 marks India's first complete effort to create a legal framework that regulates personal data collection and processing activities. The Act uses consent as its main legal basis to allow data processing while it mandates data fiduciaries to deliver privacy notices that detail their data collection practices and purposes of data collection. The Act establishes the Data Protection Board of India which will handle complaints and impose financial penalties for breaches of the law.[12] These provisions reflect a constitutional understanding that personal data belongs to the individual rather than to the entity that collects it, and that the state has an obligation to enforce the conditions under which data processing is constitutionally permissible.

The DPDPA legal framework violates constitutional requirements because its structural arrangement creates fundamental conflicts between its functioning elements and its mandated constitutional requirements. The Act establishes extensive exemptions which permit government agencies to process personal data without following its established obligations during activities related to national security and public order and their associated purposes. The Act carves out extensive exemptions which enable government entities to process personal data without adhering to established obligations.[13] The constitutional test for privacy intrusions established in Puttaswamy requires that any limitation on the right to privacy must be authorized by law, pursue a legitimate state aim, and be proportionate to that aim. The security exemptions in the DPDPA create substantial doubts about whether data processing under those exemptions can meet the three required conditions because the system lacks essential

[11]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 310-14 (Chandrachud, J.).
[12]Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).
[13]Digital Personal Data Protection Act, No. 22 of 2023, §§ 4-6 (India).

independent oversight mechanisms which include both judicial authorization requirements and independent supervisory bodies.

The structural paradox which exists within data protection systems functions because their operational procedures require organizations to conduct extensive personal data collection and processing which these systems claim to control. A regime which permits unlimited data collection yet demands only consent and notice does not resolve the fundamental constitutional issue which permits organizations to amass personal information about individuals. Zuboff's analysis of surveillance capitalism demonstrates that organizations which possess extensive behavioral data acquire a distinct kind of power which goes beyond the limits of consent-based frameworks because they can predict and change human conduct through methods which remain hidden from data subjects and which did not exist before the digital age.[14] Constitutional doctrine must eventually engage with the question of whether certain forms of data collection are categorically incompatible with the conditions of genuine autonomy, regardless of whether formal consent has been obtained.

The involvement of private entities in the collection and processing of personal data raises distinct constitutional concerns about accountability. The DPDPA applies to private data fiduciaries as well as to government entities, reflecting a recognition that the most significant threats to informational privacy in contemporary India arise from commercial data processing rather than from direct state action. This extension of data protection obligations to private actors represents a form of constitutional horizontality that is consistent with the understanding, advanced in *Puttaswamy*, that the right to privacy must be capable of generating enforceable obligations against non-state actors that exercise power over personal information.[15] Nevertheless, the DPDPA's enforcement mechanisms remain to be tested, and the practical capacity of the Data Protection Board to impose meaningful accountability on large technology companies that process vast amounts of personal data remains an open question.

IV. DIGITAL RIGHTS MANAGEMENT AND THE RECONFIGURATION OF RIGHTS AND POWER

Digital rights management technologies constitute one of the most important yet underexamined sites at which private actors exercise regulatory power that rivals governmental

[14]Zuboff, supra note 3, at 86-89.
[15]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 176 (Chandrachud, J.).

authority in its practical effect on individual rights. DRM systems are technological protection measures employed by content producers to control the conditions under which digital works can be accessed, used, copied, or distributed. In their original conception, DRM technologies were defensive instruments against copyright infringement. In their operational reality, they have become systems of pervasive private governance that determine the terms on which individuals can participate in the informational and cultural life of the digital age.[16]

The constitutional significance of DRM exists because it creates a divide between the copyright rights which the law acknowledges and the system which permits users to access protected content. Copyright doctrine exists in all legal systems because it establishes that copyright owners possess limited rights which users can exercise through various rights including their ability to make fair use of copyrighted material for research, education, commentary, and criticism work. The restrictions on copyright protection which exists in law function as legal permissions to users while they establish constitutional boundaries which protect intellectual property rights against the rights of people to express themselves and access information and engage in public discussions.[17]

The difficulty that DRM creates for this constitutional balance is that technical systems do not implement the qualifications and limitations built into legal copyright. The analysis by Lawrence Lessig about code as law shows that DRM technologies establish private control over information access because they encode copyright owner's preferred usage restrictions into content delivery systems which prevent users from exercising their copyright law rights.[18] Timothy Armstrong has shown how this asymmetry functions to deny users their right to fair use according to its established process because operations barred by DRM protection hold no legal standing according to fair use standards which require contextual assessment.[19]

The usage of algorithms to replace judicial decisions creates essential constitutional problems which threaten both the rule of law and the principle of separation of authorities. Democratic societies require constitutional governance, which mandates that authorities must gain public approval to use their power over citizens, while using clear standards, and independent judicial bodies must conduct thorough assessments of their actions. The DRM systems implemented

[16]Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 Harv. J.L. & Tech. 49, 50 (2006).
[17]Armstrong, supra note 16, at 56-57.
[18]Lessig, supra note 4, at 169-73.
[19]Armstrong, supra note 16, at 68-70.

by technology companies operate under Lessig's framework, which allows them to replace all existing enforcement mechanisms with their own private authority systems.[20] The result is that individual users are subject to restrictions on their access to knowledge and culture that are more absolute than anything the law authorizes, without any of the procedural safeguards that the law requires before those restrictions can be imposed.

The privacy dimensions of DRM compound these constitutional concerns. Many DRM systems require users to authenticate their identity and device before permitting access to protected content, and in the process collect and transmit personal data about user identity, device characteristics, and behavioral patterns to content providers or their licensees.[21] This surveillance of reading, viewing, and listening habits constitutes an intrusion into the kind of informational autonomy that the right to privacy, as understood in *Puttaswamy*, is designed to protect. The constitutional right to privacy encompasses not only the right to control the disclosure of personal information but also the right to be free from monitoring of one's intellectual and cultural activities. DRM systems that record and transmit information about the content accessed by individual users, without adequate notice or consent, implicate this dimension of the right to privacy in ways that have not yet received sustained constitutional scrutiny in India.

The constitutional challenge posed by DRM is at bottom a challenge about the scope of constitutional constraint in an era when private actors exercise power comparable to public authority. Traditional constitutional doctrine is premised on the proposition that fundamental rights constrain state action. The exercise of power by private entities, however extensive and however consequential for individual freedom, falls presumptively outside the reach of constitutional rights unless specific doctrines of horizontal application extend constitutional obligations to private actors.[22] Digital constitutionalism, as a normative framework, demands that this boundary be reconsidered. Where private technological infrastructures effectively determine the conditions under which individuals can exercise constitutional freedoms, including the freedom of expression, the right to access information, and the right to privacy, the constitutional values that those freedoms protect demand that some form of accountability mechanism be available. This may take the form of horizontal application of constitutional rights, legislative prescription of minimum standards for DRM design, or regulatory oversight

[20]Lessig, supra note 4, at 130-35.
[21]Zuboff, supra note 3, at 98-103.
[22]Celeste, supra note 2, at 82-84.

of the terms on which private actors deploy access control technologies. What it cannot take is the form of constitutional indifference to private power of this magnitude.

V. CONSTITUTIONAL CHALLENGES OF DIGITAL GOVERNANCE IN INDIA

India presents a particularly instructive context for analyzing the constitutional challenges of digital governance. The country has transformed its entire government operations through digitalization during the last ten years which involved implementing extensive technology systems for identity verification and welfare delivery and financial inclusion and law enforcement and administrative management. The systems have created constitutional disputes which have examined whether Indian constitutional law can effectively safeguard personal rights against government use of digital authority.

The Aadhaar biometric identification system has been the most consequential site of constitutional contestation over digital governance in India. The Aadhaar system started as a voluntary welfare targeting tool which later became a compulsory requirement for accessing multiple government services and private financial products. The system operates by collecting biometric data from all Indian residents who enroll in the program which main database is controlled by the Unique Identification Authority of India.[23] The Supreme Court case from 2018 which challenged the constitutionality of this system reached a Supreme Court hearing that resulted in a divided decision where the five-judge panel confirmed the Aadhaar Act's constitutional validity by a four-to-one vote while Justice Chandrachud presented a comprehensive dissent which disputed both the legal process and the fundamental constitutionality of the biometric identification system.

Justice Chandrachud's dissent in the Aadhaar Case has proved prescient as an analysis of the structural constitutional risks of data-driven governance. The Aadhaar framework established surveillance state conditions because it linked biometric authentication with increasing government services which created a system that continuously observed how people interacted with public institutions while lacking proper legal protections against abuse.[24] The majority of the court stated that authentication records should not create a surveillance risk because the system did not retain these records after completing verification, but Justice Chandrachud rejected this explanation because he found it both technically wrong and constitutionally weak

[23]Aadhaar Case, (2019) 1 SCC 1, ¶ 120 (Sikri, J.).
[24]Aadhaar Case, (2019) 1 SCC 1, ¶¶ 412-15 (Chandrachud, J., dissenting).

despite its factual correctness. The constitutional concern with extensive biometric identification develops through its permanent system that enables mass surveillance, which extends beyond its current implementation.

The Aadhaar Case also illuminated the constitutional problem of what might be called the knowledge asymmetry of digital governance. The government possessed detailed technical knowledge about the capabilities, vulnerabilities, and operational parameters of the Aadhaar system that individual petitioners and their counsel could not fully access or effectively challenge. This epistemic inequality between the state and the individual in the context of complex technical systems is not a contingent feature of the Aadhaar controversy but a structural characteristic of data-driven governance generally.[25] Constitutional doctrine that presupposes rough equality of information between the parties to a constitutional dispute will be systematically disadvantaged in addressing the constitutional dimensions of technical systems whose operation is opaque to non-specialists.

The enactment of the DPDPA represents a legislative response to the constitutional mandate established in *Puttaswamy* for comprehensive data protection. The Act's creation of the Data Protection Board of India as an adjudicatory body for data protection disputes, its specification of data principal rights including the right to access, correction, and erasure of personal data, and its imposition of financial penalties on data fiduciaries for violations of the Act's requirements each represent concrete operationalizations of the constitutional value of informational privacy.[26] The Board's effectiveness in providing genuine constitutional protection for data principals will depend critically on whether it exercises its powers with sufficient independence from the executive branch, given that the Act vests significant appointment and supervisory powers in the Central Government.

The Indian digital governance system faces a constitutional problem because of private sector participation which existing legal rules do not effectively handle. The telecommunications sector and major technology platforms together with financial service companies handle vast amounts of personal data about Indian citizens. The DPDPA establishes accountability requirements for private data fiduciaries yet its enforcement systems lack the necessary resources to match the operational scale and advanced capabilities of major technology firms.[27]

[25]Zuboff, supra note 3, at 143-47.
[26]Digital Personal Data Protection Act, No. 22 of 2023, § 18 (India).
[27]Digital Personal Data Protection Act, No. 22 of 2023, §§ 8, 10 (India).

Constitutional accountability in data governance public-private partnerships requires more than extending legal obligations to private entities because it needs institutional systems that can effectively control how private entities use public authority. India's experience with digital governance demonstrates that constitutional adaptation to the digital era needs continuous work which judges and legislative bodies must provide through multiple legal decisions and new laws. Digital technology implementation in governance systems creates constitutional issues that need new legal solutions. The Puttaswamy case establishes foundational principles which courts and legislators and regulators need to apply through extended constitutional examination of specific digital governance problems. Digital constitutionalism functions as a normative framework which requires constitutional values to govern digital systems according to this ongoing project.[28]

VI. CONCLUSION

The digital era has transformed the conditions under which constitutional values are exercised, protected, and threatened. The constitutional challenges analyzed in this article, from the normalization of surveillance as an administrative technique to the structural paradoxes of data protection regimes to the private governance of informational access through DRM, share a common characteristic: they arise from the operation of technical systems that exercise power over individuals without the formal markers of governmental authority that constitutional doctrine traditionally requires before its protections are engaged. Digital constitutionalism, as a normative framework and an emerging field of doctrinal development, insists that constitutional values must follow power wherever it is effectively exercised, regardless of whether the actor wielding that power bears the formal attributes of a state.

The recognition of privacy as a fundamental right in *Puttaswamy* is the most significant constitutional development in India in the digital era, but it is a beginning rather than a resolution. Its implications for data protection, biometric governance, algorithmic decision-making, and the regulation of private technological power remain incompletely worked out. The enactment of the DPDPA provides a legislative framework for operationalizing the constitutional mandate of informational privacy, but significant structural questions about governmental exemptions, enforcement capacity, and the independence of the Data Protection

[28]Aadhaar Case, (2019) 1 SCC 1, ¶¶ 204-08 (Chandrachud, J., dissenting).

Board require ongoing constitutional scrutiny.[29]

Digital rights management illustrates the broader principle that constitutional concern cannot be confined to formal state action in a world where private actors exercise regulatory functions through technical design. The constitutional values of expressive freedom, access to knowledge, and informational autonomy are all implicated by DRM systems that operate beyond the reach of traditional constitutional doctrine. The normative framework of digital constitutionalism demands that these values generate enforceable constraints on private as well as public power, though the specific institutional mechanisms through which this constraint is achieved remain contested and require further development.

The Indian constitutional experience teaches valuable lessons to the worldwide effort of establishing digital constitutionalism. India's combination of a rights-protective constitutional text, an activist judiciary, a rapidly expanding digital infrastructure, and a large and diverse population makes its constitutional engagement with digital governance particularly rich as a site of doctrinal development and normative contestation. The challenges India faces, from balancing welfare delivery efficiency against privacy rights to managing the constitutional implications of public-private data partnerships, exist in other countries but they show their most urgent form in India.

The digital age demands a complete transformation of constitutional law to maintain its foundational values. The core commitments of dignity, liberty, autonomy, and democratic accountability remain unchanged yet need continuous updates to their protective systems because digital power generates new threats. Digital constitutionalism as defined by Redeker Gill Gasser and Celeste has become a global legal standard which judicial systems and legislative bodies now adopt as the digital age requires constitutional systems that match its technological advancements.[30]

[29]Celeste, supra note 2, at 90.
[30]Redeker, Gill & Gasser, supra note 1, at 316.