FROM FUNDAMENTAL RIGHTS TO DIGITAL RIGHTS: DIGITAL CONSTITUTIONALISM OF DATA PRIVACY IN INDIA

Mr. Rishav Dogra, PhD Research Scholar, Himachal Pradesh University, H.P.

Prof. (Dr.) D.P. Verma, Professor, Himachal Pradesh University Regional Centre, Dharamshala, H.P.

ABSTRACT

The Indian Constitution, a remarkable synthesis of aspirational rights and institutional checks, has proven to be a living document dynamic and responsive to changing socio-political realities. In the 21st century, data has become the new oil of governance and economy, raising urgent constitutional questions concerning privacy, surveillance, and digital autonomy. This paper examines the evolution of the Indian Constitution as a living document through the lens of data privacy jurisprudence. It analyzes landmark judicial pronouncements, particularly Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), and legislative interventions such as the Digital Personal Data Protection Act, 2023 (DPDP Act). The analysis includes an extensive critique of the Digital Personal Data Protection Act, 2023, and a wide comparative study referencing GDPR, POPIA, and the United States' sectoral privacy regime. The paper concludes with policy recommendations to strengthen India's digital constitutionalism, including an independent data protection authority, algorithmic transparency mandates, and constitutional safeguards for AI governance. Further, it explores how constitutional principles liberty, dignity, and proportionality interact with technological advancements and state surveillance. Drawing comparative insights from the European Union's GDPR, the United States' sectoral privacy model, and South Africa's constitutional framework, the paper concludes that India's living Constitution must continue evolving to protect the informational autonomy of individuals in a data-driven society.

I. Introduction

The Constitution of India, brought into force in 1950, was never intended to function as a rigid or inflexible legal document. Instead, its framers envisioned it as a dynamic and transformative charter capable of evolving with societal progress. Dr. B.R. Ambedkar famously encapsulated this philosophy by noting that the Constitution is "a living organism" that must continually adapt to changing circumstances.1 The concept of fundamental rights under the Indian Constitution was originally framed in a pre-digital context, focusing primarily on civil liberties such as equality, freedom of speech, and personal liberty. However, the advent of the digital age has transformed the nature of rights, particularly concerning informational privacy and data protection.

With the exponential growth of data collection, surveillance technologies, and digital governance, the traditional interpretation of fundamental rights has proven inadequate. The need to reinterpret constitutional protections in light of technological advancements has led to the emergence of "digital rights" as an extension of fundamental rights.

India's constitutional jurisprudence has gradually evolved to accommodate these changes, culminating in the judicial recognition of privacy as a fundamental right. This transition reflects a broader shift from state-centric governance to individual-centric digital autonomy.

A watershed moment in this evolution came with *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which the Supreme Court unequivocally recognized privacy as a fundamental right protected under Articles 14, 19, and 21.[2] This decision reaffirmed that the Constitution must be interpreted as a living document capable of addressing the complex realities of the digital era.

- **Conceptual Foundation: What "Digital Constitutionalism" Means for India**

"Digital constitutionalism" refers to the application of **constitutional values dignity, liberty, equality, rule of law, and accountability within the digital ecosystem**. In the Indian context, this transformation is not merely regulatory but **normative and structural**, grounded in Part III of the Constitution and judicial interpretation.

[1] Dr. B.R. Ambedkar, Constituent Assembly Debates (1949)
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

The Supreme Court in Justice K.S. Puttaswamy v. Union of India laid the doctrinal foundation by affirming that privacy is intrinsic to life and liberty. The challenge now is to **translate this constitutional recognition into an operational digital rights framework** that governs both state and private actors.

Indian digital constitutionalism must therefore evolve as:

- **Rights-centric (not merely compliance-driven)**
- **Technology-neutral but future-ready**
- **Balanced between innovation and civil liberties**

Strengthening the Constitutional Architecture of Digital Rights

(a) Explicit Recognition of Digital Rights

While privacy has been recognized judicially, India still lacks explicit articulation of **digital rights such as:**

- Right to informational self-determination
- Right to data portability
- Right against algorithmic profiling
- Right to encryption and anonymity

A progressive approach would involve **judicial expansion and legislative codification** of these rights, aligning them with Articles 14, 19, and 21.

(b) Embedding Proportionality as a Constitutional Standard

The proportionality doctrine, crystallized in Justice K.S. Puttaswamy v. Union of India, must become the **default test for all digital intrusions**, including surveillance, data collection, and content regulation.

This requires:

- Clear statutory thresholds for state action
- Mandatory judicial or independent authorization for surveillance
- Periodic review and sunset clauses for intrusive measures

Without strict proportionality, digital governance risks drifting into **constitutional overreach**.

II. Historical Evolution of Living Constitutionalism in India

The notion of a "living constitution," though widely associated with American jurisprudence and articulated by jurists such as Justice Oliver Wendell Holmes and Justice Brennan,[3] found early resonance within India's constitutional development. The Supreme Court's landmark decision in *Kesavananda Bharati v. State of Kerala* articulated the basic-structure doctrine, affirming that while the Constitution can evolve, its foundational principles must remain intact.[4]This doctrine has since served as a structural anchor for constitutional interpretation.

India's foundational constitutional thought was shaped by its colonial experience, which demonstrated the dangers of unchecked state authority. Constituent Assembly debates reflect a clear awareness that liberty required meaningful protections against state intrusion. Although the Constitution does not explicitly enumerate a right to privacy, members of the Assembly acknowledged that privacy was embedded within the broader protections of personal liberty under Article 21.[5]

As India transitioned from a postcolonial democracy to a digital polity, the imperative for constitutional flexibility intensified. Over time, constitutional interpretation responded to new social and technological contexts expanding the meaning of rights relating to equality, dignity, and eventually privacy. This demonstrates how judicial creativity and societal necessity continually shape constitutional meaning.

III. The Doctrine of Living Constitution in Judicial Interpretation

The Supreme Court has consistently adopted a purposive and evolutionary interpretative approach, enabling constitutional rights to remain meaningful in changing times. A seminal

[3] Oliver Wendell Holmes, "The Path of the Law," Harv. L. Rev. (1897)
[4] Kesavananda Bharati v. State of Kerala, AIR 1973 SC 1461
[5] Constituent Assembly Debates (1948).

example is *Maneka Gandhi v. Union of India*, where the Court held that the right to travel abroad falls within the ambit of personal liberty under Article 21.[6] In the same judgment, the Court broadened due-process protections by declaring that "procedure established by law" must be "right, just, and fair."

This dynamic interpretive approach reflects the Constitution's living character. The Court has relied on the doctrine of constitutional morality to reinterpret rights in light of contemporary social realities. For example, in *Navtej Singh Johar v. Union of India*, the Court decriminalized same-sex relations, emphasizing dignity and autonomy as constitutional values.[7] Similarly, in *Joseph Shine v. Union of India*, the Court struck down the adultery provision as unconstitutional, underscoring equality and personal autonomy.[8]

Collectively, these decisions represent a steady expansion of constitutional protections related to dignity, autonomy, and privacy principles that now form the basis of India's jurisprudence on data protection and digital rights.

IV. The Emergence of the Right to Privacy: From *Gobind* to *Puttaswamy*

The constitutional journey toward recognizing privacy as a fundamental right in India has been incremental and complex. In its early decisions, the Supreme Court adopted a narrow understanding of privacy. In *M.P. Sharma v. Satish Chandra*, the Court held that the Constitution did not expressly confer a right to privacy and therefore declined to read one into it.[9] This restrictive view was reiterated in *Kharak Singh v. State of Uttar Pradesh*, where the majority again refused to recognize privacy as a constitutionally protected value.[10] However, Justice Subba Rao's influential dissent argued that personal liberty necessarily encompassed the sanctity of the home, family life, and personal freedom.

As constitutional jurisprudence evolved, subsequent decisions began expanding the scope of liberty under Article 21. In *Gobind v. State of Madhya Pradesh*, the Court cautiously acknowledged privacy as a "penumbral right" emerging from the constitutional guarantee of

[6] Maneka Gandhi v. Union of India, AIR 1978 SC 597
[7] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1
[8] *Joseph Shine v. Union of India*, (2019) 3 SCC 39
[9] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300
[10] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295

liberty, noting that the contours of privacy would evolve on a case-by-case basis.[11] This judicial openness set the stage for doctrinal development.

The transformation accelerated with *Maneka Gandhi*, which integrated privacy with notions of fairness, reasonableness, and due process, thus broadening the reach of Article 21. Toward the end of the twentieth century, cases such as *R. Rajagopal v. State of Tamil Nadu* established informational privacy as essential to personal autonomy,[12] while *People's Union for Civil Liberties (PUCL) v. Union of India* highlighted the dangers of unchecked surveillance, laying down procedural safeguards for telephone tapping.[13] These decisions collectively prepared the groundwork for *Puttaswamy*, where privacy was finally elevated to an explicit fundamental right.

V. *Puttaswamy* Judgment: A Constitutional Renaissance

The nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a transformative moment in Indian constitutional law. In this landmark judgment, the Court unanimously affirmed that privacy is a fundamental right intrinsic to human dignity and liberty, protected across Articles 14, 19, and 21.[14] Justice D.Y. Chandrachud, writing for the majority, emphasized that privacy forms the basis of individual autonomy and is indispensable to the exercise of constitutionally guaranteed freedoms.

Importantly, *Puttaswamy* overruled both *M.P. Sharma* and *Kharak Singh*, harmonizing privacy with India's commitment to transformative constitutionalism. The judgment explicitly recognized **informational privacy** including the right to control one's personal data as a central component of individual autonomy in the digital age.

The Court also drew from international human-rights instruments such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, underscoring privacy's global recognition as a fundamental right.[15]

A significant contribution of *Puttaswamy* is the adoption of a **three-fold test** for assessing

[11] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148
[12] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632
[13] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301
[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1
[15] Universal Declaration of Human Rights, art. 12; ICCPR, art. 17

privacy restrictions:

1. **Legality** any intrusion must be backed by law;
2. **Legitimate aim** the objective must be necessary and aligned with a valid state purpose;
3. **Proportionality** the measure must be narrowly tailored and be the least restrictive means available.[16]

This proportionality framework now forms the constitutional benchmark for evaluating surveillance, data-protection laws, and state action involving personal data.

VI. Informational Privacy and the Digital State

In the era of big data, privacy transcends mere physical or spatial protection. **Informational privacy** concerns an individual's ability to control access to and the use of personal data. With the proliferation of digital platforms, biometric systems, and algorithmic governance, individuals increasingly leave behind extensive digital footprints.

The Aadhaar project highlighted this tension between administrative efficiency and personal privacy. In the Aadhaar ("*Puttaswamy II*") decision, the Supreme Court upheld the Aadhaar Act but introduced strict safeguards regarding purpose limitation, data retention, and proportionality.[17]

Government-led digital initiatives such as CoWIN for vaccination management, DigiLocker for digital documentation, and facial-recognition databases used by law-enforcement agencies raise pressing concerns regarding consent, transparency, and accountability. The Supreme Court has emphasized that **informational self-determination** the ability to control one's data is essential to personal dignity in a democratic society.[18] Without robust safeguards, the architecture of the digital state risks shifting toward mass surveillance.

VII. Data Privacy and Surveillance: Constitutional and Policy Challenges

Rapid digitalization has blurred the line between welfare and surveillance in India. Large-scale systems such as the Central Monitoring System (CMS), NATGRID, and automated facial-

[16] *Puttaswamy*, (2017) 10 SCC 1
[17] *K.S. Puttaswamy v. Union of India* ("Aadhaar"), (2019) 1 SCC 1
[18] Id

recognition technologies collect vast quantities of personal data without adequate legislative oversight. In *PUCL v. Union of India* (the "Telephone Tapping Case"), the Supreme Court held that surveillance without procedural safeguards violates Article 21.[19] Despite this, data interception often occurs under broad executive discretion vested in antiquated statutes such as the Telegraph Act, 1885, and the Information Technology Act, 2000.

For decades, the absence of a comprehensive data-protection law resulted in regulatory fragmentation and a lack of uniform standards. Civil-society groups and scholars have repeatedly warned that opaque data-sharing arrangements between government departments and between the state and private intermediaries pose serious constitutional risks. Several commentators argue that the constitutional balance between **national security** and **individual privacy** has increasingly tilted in favor of the state, necessitating renewed emphasis on rights-based governance.[20]

Moreover, private-sector entities such as financial-technology platforms, e-commerce companies, and social-media corporations accumulate extensive personal data for commercial purposes. This has revived debates on the **horizontal application of fundamental rights**, particularly whether constitutional values such as privacy and dignity should bind corporations when processing user data.

VIII. The Digital Personal Data Protection Act, 2023 (DPDP Act): A Detailed Examination

The Digital Personal Data Protection Act, 2023 (DPDP Act) constitutes India's first comprehensive statutory framework dedicated exclusively to the regulation of personal data. The Act introduces and defines several foundational concepts such as "data fiduciary," "data principal," "consent," and "legitimate use" which structure the operation of India's emerging data-protection regime.[21] Although the DPDP Act draws conceptual and structural influence from the European Union's General Data Protection Regulation (GDPR), scholars and jurists have raised concerns regarding its constitutional soundness, particularly in relation to Articles 14, 19, and 21 of the Indian Constitution.[22]

[19] *PUCL v. Union of India*, (1997) 1 SCC 301
[20] Gautam Bhatia, *Privacy, National Security, and the Indian Constitution*, Indian Const. L. & Phil. (2020)
[21] Digital Personal Data Protection Act, No. 22 of 2023, § 2 (India).
[22] See *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

a) **Strengths of the DPDP Act** : The DPDP Act incorporates a notice-and-consent mechanism that seeks to empower individuals by ensuring transparency in the processing of personal data. It further prescribes statutory penalties for data breaches, thereby creating deterrence for wrongful data handling. A significant institutional innovation under the Act is the establishment of the Data Protection Board of India, envisaged as a specialized body to adjudicate violations and enforce compliance.[23] Section 8 of the DPDP Act establishes the principles of data minimization and purpose limitation doctrinally aligned with the proportionality framework articulated by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* ("Puttaswamy I"). These safeguards demonstrate an attempt to anchor statutory data protection within constitutionally recognized constraints.

b) **Limitations and Areas of Constitutional Concern**

Despite its strengths, the DPDP Act contains broad state-centric exemptions under Section 17, which permit the government to process personal data in the "interest of sovereignty, security, or public order."[24] Such provisions grant sweeping discretionary authority to the executive and risk diluting the fundamental right to privacy recognized in *Puttaswamy I*. Additionally, unlike the EU model, India's framework lacks an independent, constitutionally insulated data authority potentially undermining oversight and accountability in situations involving sensitive or large-scale data processing.[25]

c) **Comparative Deficiencies**

When compared with global standards, the DPDP Act exhibits several gaps. Unlike the GDPR, which codifies rights such as data portability and the "right to be forgotten," the Indian Act treats these rights as conditional or discretionary in nature.[26] It also offers limited protections regarding cross-border data transfer, and it does not impose explicit obligations relating to algorithmic transparency or automated decision-making an omission significant in the context of AI-driven governance. Consequently, while the DPDP Act marks an

[23] Digital Personal Data Protection Act, No. 22 of 2023, ch. V (establishing the Data Protection Board of India)
[24] Digital Personal Data Protection Act, No. 22 of 2023, § 17
[25] See generally Regulation (EU) 2016/679, General Data Protection Regulation, art. 51 (establishing independent supervisory authorities)
[26] Id. at arts. 17, 20.

important legislative milestone, it remains a relatively limited response to India's constitutional obligations in the digital age.[27]

IX. Comparative Constitutional Analysis

a) European Union & United States

The European Union provides the most robust constitutional and statutory protection for informational privacy. The Charter of Fundamental Rights guarantees both privacy (Article 7) and data protection (Article 8) as independent rights. These guarantees are operationalized through the GDPR, which enshrines principles of lawfulness, fairness, purpose limitation, and accountability. In *Schrems II*, the Court of Justice of the European Union (CJEU) invalidated the EU–US Privacy Shield, stressing that international data transfers require equivalent levels of protection in the receiving jurisdiction.[28] By contrast, India's DPDP Act delegates cross-border transfer decisions to the central government, raising questions about adequacy if assessed under EU standards. The United States follows a fragmented, sectoral model of privacy regulation through statutes such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm–Leach–Bliley Act (GLBA).[29] The U.S. Constitution does not explicitly enumerate a right to privacy; instead, it has been inferred from the "penumbras" of various constitutional provisions, as articulated in Griswold v. Connecticut.[30] Landmark cases such as Carpenter v. United States and Riley v. California reflect the Supreme Court's willingness to extend constitutional protections into the digital domain by recognizing the sensitivity of location data and smartphone contents.[31] India's living-constitution model aligns more closely with this interpretative approach while rooting privacy directly in the text through Articles 14, 19, and 21.

X. Theoretical Dimensions: Constitutional Morality, Proportionality & Data Autonomy

Dr. B.R. Ambedkar's formulation of constitutional morality underscores the need for citizens

[27] For critical commentary, see Gautam Bhatia, *The DPDP Act and the Constitutional Right to Privacy*, INDIAN CONST. L. & PHIL. BLOG (2023).
[28] Case C-311/18, *Data Protection Comm'r v. Facebook Ireland Ltd.*, 2020 E.C.R. (Schrems II).
[29] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809
[30] *Griswold v. Connecticut*, 381 U.S. 479, 484–85 (1965).
[31] *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014)

and institutions to act in accordance with constitutional values rather than fluctuating public sentiment.[32] In the domain of data privacy, this concept demands restraint on state surveillance and adherence to principles of dignity and autonomy. The Supreme Court reaffirmed the centrality of constitutional morality in Navtej Singh Johar v. Union of India, emphasizing that rights adjudication must not be swayed by majoritarian impulses. This principle is equally applicable to digital-governance frameworks.

a) The Proportionality Doctrine

The proportionality test, articulated in Puttaswamy I and refined in Modern Dental College v. State of Madhya Pradesh, requires that any intrusion into privacy satisfy legality, necessity, and minimal impairment.[33] Applied to data-processing practices, this doctrine ensures that both governmental surveillance and corporate data collection remain subject to constitutional constraints. It also provides a judicial mechanism for evaluating the legality of automated or algorithmic decision-making systems.

b) Data Autonomy and Digital Personhood

Informational privacy extends traditional liberal notions of autonomy into digital environments. Scholars such as Daniel Solove argue that privacy revolves around control over one's personal information rather than mere secrecy.[34] The Supreme Court's recognition of privacy as intrinsic to dignity effectively affirms a concept of "digital personhood," wherein individuals possess inherent rights over their data identity. Ensuring informational autonomy is therefore central to fulfilling the constitutional guarantee of dignity under Article 21.

Comparative Analysis: India vs GDPR

Aspect	**GDPR (EU)**	**India (DPDP Act, 2023)**
Philosophy	Rights-based, individual-centric	Balanced but state-inclined
Legal Basis	Multiple bases (consent, contract, legitimate interest)	Primarily consent-driven

[32] 11 CONSTITUENT ASSEMBLY DEBATES 38 (1949) (statement of Dr. B.R. Ambedkar).
[33] *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353
[34] DANIEL J. SOLOVE, *Understanding Privacy* 1–15 (Harv. Univ. Press 2008).

Aspect	**GDPR (EU)**	**India (DPDP Act, 2023)**
Regulator	Independent DPAs	Data Protection Board (executive influence concerns)
Penalties	Severe, turnover-based	Financial penalties but less stringent
State Exemptions	Limited, proportionate	Broad exemptions for government
Data Localization	Not mandatory	Selective approach
Rights Scope	Extensive (portability, objection, etc.)	More limited

Key Observations

- India's framework is **less rights-intensive** compared to GDPR
- Enforcement in India lacks **institutional independence**
- State power in India is **less constrained** than in the EU model

Key recommendations for strengthening India's digital constitutionalism include:

1. **Creation of an independent Data Protection Authority** insulated from executive influence.
2. **Mandatory algorithmic transparency audits** for all AI systems deployed in public administration.[35]
3. **Integration of privacy-by-design principles** into all government-operated digital platforms.
4. **Comprehensive legislative harmonization** aligning the DPDP Act with the Information Technology Act and future AI-specific regulations.
5. **Explicit constitutional or judicial recognition** of informational self-determination as

[35] See generally Justice B.N. Srikrishna Committee, *Report of the Committee of Experts on Data Protection Framework for India* (2018).

a core facet of dignity.

As India aspires to leadership in the digital economy, its constitutional ethos must ensure that technological advancement strengthens not undermines liberty, accountability, and democratic values.

12. Conclusion

The Indian Constitution's vitality lies in its capacity for reinterpretation. From *Maneka Gandhi* to *Puttaswamy*, the Supreme Court has continuously expanded the horizon of fundamental rights. Data privacy epitomizes the next phase of this evolution. The Constitution, as a living document, must now safeguard individuals against informational exploitation and surveillance capitalism.

While the *Digital Personal Data Protection Act, 2023* marks legislative progress, it must operate within constitutional boundaries defined by proportionality and dignity. Comparative insights reveal that India must evolve toward a rights-centric, independent, and transparent data-protection ecosystem.

Ultimately, constitutionalism in the digital age demands not only judicial vigilance but also civic awareness. The living Constitution thrives when its citizens insist upon the inviolability of liberty even in bytes and algorithms.