THE EVOLVING DOCTRINE OF DATA PRIVACY IN INDIA: CONSTITUTIONAL FOUNDATIONS, JUDICIAL TRENDS, AND LEGISLATIVE CHALLENGES

Saurabh, Patna Law College, Patna University

ABSTRACT

The doctrine of data privacy has emerged as one of the most significant constitutionals, normative and regulatory concerns within India's evolving digital landscape. With rapid technological penetration and the proliferation of digital public infrastructure, questions regarding informational autonomy and personal data protection have become central to constitutional governance. The emergence of Aadhaar-based authentication, fintech platforms, social media ecosystems and digital health records demonstrates the growing reliance on data-driven decision-making in both public and private spheres. Against this backdrop, the recognition of the right to privacy as a fundamental right under Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a jurisprudential watershed. The judgment identified privacy as integral to dignity, autonomy and personal liberty, and articulated a proportionality-based test to assess permissible restrictions on the right.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) is India's first attempt at adopting a comprehensive data protection regime. While the Act introduces consent requirements, duties of data fiduciaries, rights of data principals and a redressal mechanism, a number of concerns remain. These include wide-ranging State exemptions, the absence of an independent supervisory authority, weak safeguards against surveillance, and limited individual remedies. When examined through the constitutional lens laid down in *Puttaswamy*, certain provisions—particularly the government's power to exempt agencies from compliance—raise serious questions regarding proportionality, accountability and procedural fairness.

A comparative examination with global standards such as the European Union's General Data Protection Regulation (GDPR) reveals structural lacunae in India's framework, particularly in areas such as purpose limitation, data minimisation, breach reporting, and cross-border data transfers. This article argues that although the DPDPA constitutes a significant step forward, its effectiveness ultimately depends on strengthening regulatory independence and embedding constitutional

safeguards into every stage of data governance. The future of India's digital constitutionalism requires a rights-centric foundation that upholds privacy not merely as a statutory measure but as an essential democratic value.

INTRODUCTION

Recent judicial developments in India have reaffirmed and expanded the constitutional contours of the right to privacy, especially in the context of digital surveillance, data protection and informational autonomy. In *Anuradha Bhasin v. Union of India* (2020), the Supreme Court held that access to the internet is integral to the freedom of speech and expression under Article 19(1)(a), emphasising that restrictions on digital communication must satisfy the tests of necessity and proportionality.[1] This principle was further strengthened in *Foundation for Media Professionals v. Union Territory of Jammu & Kashmir* (2020), where the Court insisted on periodic review of internet restrictions to prevent arbitrary curtailment.[2]

More recently, in *Puttaswamy (Aadhaar–II) Review Petitions* (2023), the Supreme Court reiterated that any State action involving large-scale data collection must be justified through a demonstrable rational nexus and minimal intrusiveness, signalling strict scrutiny of data-intensive governance.[3] In *Internet Freedom Foundation v. Union of India* (2022), the Delhi High Court raised concerns regarding indiscriminate data retention and sought justification for policies mandating prolonged storage of subscriber information by intermediaries.[4] Similarly, the Kerala High Court in *Vinu Prasad v. State of Kerala* (2023) reaffirmed that individuals retain control over their personal data and that law enforcement access must always be backed by statutory authority and proportional safeguards.[5]

These contemporary rulings illustrate a judicial insistence on constitutional guardrails in the digital era, making it clear that informational privacy cannot be subordinated to administrative convenience or technological expediency. As India navigates an increasingly data-driven governance ecosystem, these decisions underscore the relevance of privacy as a foundational right.

[1] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[2] *Foundation for Media Professionals v. Union Territory of Jammu & Kashmir*, (2020) 5 SCC 698.
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Review)*, Review Petitions in W.P. (C) No. 494/2012, order dated Jan. 2023.
[4] *Internet Freedom Foundation v. Union of India*, W.P.(C) 8601/2018, Delhi High Court (2022).
[5] *Vinu Prasad v. State of Kerala*, 2023 SCC OnLine Ker 211.

Against this evolving jurisprudence, the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant legislative development. Yet, questions remain about whether the Act aligns with constitutional requirements articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* particularly regarding legality, necessity and proportionality. With both State and private actors becoming major processors of personal data, the need for a balanced, rights-centric data protection regime has become more urgent than ever.

This article therefore situates the DPDPA within contemporary judicial developments, examining how Indian courts are shaping the future of digital constitutionalism while evaluating whether the new statutory regime adequately protects informational autonomy.

HISTORICAL DEVELOPMENT OF PRIVACY JURISPRUDENCE IN INDIA

The evolution of privacy jurisprudence in India reflects a gradual but significant transformation in constitutional interpretation. In its early approach, the Supreme Court declined to recognise privacy as a protected fundamental right, most notably in *M.P. Sharma v. Satish Chandra*[6] and later in *Kharak Singh v. State of Uttar Pradesh*.[7] These decisions adopted a narrow understanding of personal liberty, confining it to physical restraints and rejecting broader notions of informational or decisional autonomy.

Over time, however, judicial reasoning began to shift. Subsequent constitutional adjudication increasingly embraced a more expansive reading of Article 21, acknowledging that personal liberty cannot be meaningfully protected without safeguarding individual autonomy and private life. This doctrinal journey reached its decisive moment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge bench unanimously held that the right to privacy is an inherent component of dignity, freedom and personal liberty under Article 21.[8] The judgment marked a constitutional turning point, firmly embedding privacy within India's rights framework and laying the foundation for contemporary data-protection jurisprudence.

CONSTITUTIONAL FOUNDATIONS AND THE PROPORTIONALITY FRAMEWORK

The constitutional grounding of the right to privacy in India was firmly articulated in the *Justice*

[6] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[7] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

K.S. Puttaswamy (Retd.) v. Union of India decision, which clarified that privacy is an indispensable element of human dignity and personal liberty protected under Article 21.[9] The Court observed that modern democratic governance requires safeguarding individuals from both State intrusions and excessive data collection by private actors. By embedding privacy within the broader spectrum of fundamental rights, the judgment established a rights-based framework that governs all subsequent legislative and executive actions affecting personal data.

A key contribution of *Puttaswamy* is the adoption of a structured proportionality analysis to evaluate the permissibility of restrictions on privacy. The Court held that any interference must satisfy four cumulative conditions:

1. the existence of a valid law authorising the measure;
2. a legitimate State aim demonstrating the necessity of such interference;
3. a proportional relationship between the objective pursued and the means employed, ensuring the least restrictive alternative is adopted; and
4. procedural safeguards that prevent arbitrary or excessive exercise of power.[10]

This proportionality standard not only aligns Indian constitutional law with global human rights jurisprudence but also provides a rigorous test for assessing modern data-governance frameworks. It serves as a central benchmark in evaluating whether emerging regulatory models including the Digital Personal Data Protection Act, 2023 adequately respect informational autonomy while balancing competing State interests.

LEGISLATIVE FRAMEWORK: DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) represents India's first comprehensive attempt to codify a statutory framework governing the collection, processing and protection of personal data. The Act conceptualises a rights-based data governance model by imposing a series of obligations on "data fiduciaries" and corresponding entitlements on

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[10] Id. at ¶¶ 180–182.

"data principals." At its core, the DPDPA requires that processing of personal data be grounded in valid consent, which must be free, specific, informed and unambiguous.[11] The statute also recognises the principle of data minimisation by mandating that only such data as is necessary for a lawful purpose may be collected or processed. Additionally, the Act obligates data fiduciaries to provide clear and accessible notices, maintain reasonable security safeguards, ensure accuracy of data, and establish grievance-redressal mechanisms to address violations or misuse.[12]

Beyond individual rights and fiduciary obligations, the Act introduces the institutional framework of the **Data Protection Board of India**, envisioned as a regulatory body responsible for adjudicating breaches, enforcing compliance and imposing penalties. Although the Board represents an important step towards administrative oversight, concerns persist regarding its independence and operational autonomy, particularly because its composition and functioning are subject to significant executive control.[13]

One of the most contentious aspects of the DPDPA is the breadth of exemptions available to the Central Government. Under Section 17, the government may exempt its agencies from the application of key provisions of the Act for reasons such as national security, public order or prevention of offences. These exemptions permit extensive derogations from core safeguards—including consent requirements, storage limitations and individual rights—raising serious questions about proportionality, necessity and the potential for overbroad State surveillance.[14] When assessed in light of the constitutional framework articulated in *Puttaswamy*, such wide discretionary powers may undermine the very rights that the Act purports to protect, thereby creating a tension between statutory design and constitutional expectations.[15]

CHALLENGES IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Despite representing a major legislative milestone, the Digital Personal Data Protection Act, 2023 (DPDPA) contains several structural and normative gaps that raise significant constitutional and regulatory concerns. One of the foremost challenges lies in the expansive

[11] Digital Personal Data Protection Act, 2023, § 6 (Consent Requirements).
[12] Id. §§ 7–9 (Notice Obligations, Data Minimisation, Security Safeguards).
[13] Id. §§ 19–21 (Establishment and Functions of the Data Protection Board of India).
[14] Id. § 17 (Government Exemptions).
[15] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

exemptions available to the Central Government under Section 17, which authorise the State to bypass core obligations relating to consent, notice, data minimisation and storage limitations.[16] These exemptions justified on grounds such as national security, sovereignty and public order create a broad zone of executive discretion, potentially facilitating intrusive surveillance practices without adequate procedural safeguards. When evaluated against the proportionality framework laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, such unrestricted powers risk undermining informational autonomy and the fundamental right to privacy.[17]

A second challenge concerns the institutional design of the Data Protection Board of India, which is tasked with adjudicating breaches and enforcing compliance. Although conceived as the central regulatory body, the Board's independence is potentially compromised because its appointment, tenure and removal are largely controlled by the Central Government.[18] International best practices, including those embedded in the European Union's GDPR, emphasise the need for independent supervisory authorities insulated from political influence a standard the DPDPA does not fully satisfy.[19] The absence of structural autonomy raises doubts about the Board's capacity to enforce the Act impartially, especially in cases involving State actors.

Another area of concern is the limited scope of individual rights under the Act. Compared to global regimes, the DPDPA offers a narrower set of entitlements to data principals, most notably lacking expansive rights such as data portability and a robust right to object to processing.[20] The Act also places substantial onus on individuals to monitor and enforce their own rights, without creating strong obligations of transparency on data fiduciaries. This asymmetry may weaken accountability and inhibit individuals from meaningfully exercising control over their personal data.

Additionally, the framework for **cross-border data transfers** relies primarily on government notifications that specify permitted jurisdictions, rather than objective adequacy assessments

[16] Digital Personal Data Protection Act, 2023, § 17 (Exemptions for Government Agencies).
[17] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[18] Digital Personal Data Protection Act, 2023, §§ 19–21 (Constitution and Functions of the Data Protection Board of India).
[19] General Data Protection Regulation, art. 52 (Requirement of Independent Supervisory Authorities).
[20] Compare Digital Personal Data Protection Act, 2023, § 12, with General Data Protection Regulation, arts. 15–22.

based on data-protection standards.[21] This creates uncertainty for international data flows and may not provide adequate protection against misuse or unauthorised access by foreign entities.

Collectively, these challenges underscore the tension between the Act's stated commitment to privacy protection and its embedded mechanisms that allow significant executive discretion. Unless supplemented by stronger safeguards, transparent procedures and genuinely independent regulatory oversight, the DPDPA may fall short of delivering the rights-centric data-protection framework envisioned by the Indian Constitution.

COMPARATIVE PERSPECTIVE WITH THE GDPR

A comparative analysis between the Digital Personal Data Protection Act, 2023 (DPDPA) and the European Union's General Data Protection Regulation (GDPR) reveals significant divergences in regulatory philosophy, institutional design and individual rights. The GDPR, widely regarded as the most comprehensive global data-protection framework, is built upon foundational principles such as lawfulness, fairness, transparency, purpose limitation and data minimisation.[22] These principles not only guide data-processing activities but also operate as enforceable obligations subject to strong oversight by independent supervisory authorities. In contrast, the DPDPA, while drawing inspiration from several GDPR concepts, adopts a more limited and State-centric approach that prioritises administrative flexibility over stringent individual rights protections.

One of the most notable distinctions concerns the scope of individual rights. Under the GDPR, data subjects enjoy a wide range of entitlements including the rights to access, rectify, erase, restrict processing and data portability.[23] The DPDPA grants only a reduced set of rights, omitting, for instance, the right to data portability and offering a more restricted version of the right to erasure. This narrower rights framework limits the ability of individuals to control the lifecycle of their personal data.

Similarly, the role and independence of regulatory authorities mark an important point of divergence. The GDPR mandates fully independent Data Protection Authorities vested with investigative, corrective and supervisory powers.[24] In contrast, the Data Protection Board of

[21] Digital Personal Data Protection Act, 2023, § 16 (Cross-Border Data Transfers).
[22] General Data Protection Regulation, art. 5 (Principles of Processing).
[23] Id. arts. 12–22 (Data Subject Rights).
[24] Id. art. 52 (Independence of Supervisory Authorities).

India, established under the DPDPA, is primarily an adjudicatory body whose constitution, functioning and administrative control lie with the Central Government.[25] This structural difference raises concerns regarding impartiality and the enforcement of privacy rights, especially in cases involving State actors.

Moreover, the GDPR establishes a rigorous regime for cross-border data transfers, allowing such transfers only to jurisdictions with an "adequacy decision" or where appropriate safeguards are in place.[26] The DPDPA, however, adopts a more discretionary framework based largely on government notifications, without requiring a substantive assessment of foreign data-protection standards.[27] This creates uncertainty in international data flows and may not ensure equivalent protection abroad.

Taken together, these distinctions underscore that while the DPDPA represents progress toward a structured data-protection regime, it lacks the robustness, rights-centric orientation and institutional independence characteristic of the GDPR. The comparison highlights areas where India's model may benefit from further refinement to ensure stronger alignment with global best practices.

CONCLUSION

The evolution of India's privacy jurisprudence, culminating in the landmark *Puttaswamy* decision, established privacy as a core constitutional value intrinsically linked to dignity and personal autonomy.[28] The Digital Personal Data Protection Act, 2023 marks a significant step toward translating this constitutional mandate into statutory form. However, the Act's effectiveness ultimately depends on whether its implementation remains faithful to the principles of necessity, proportionality and accountability articulated by the Supreme Court.

While the DPDPA introduces an organised framework for consent, fiduciary obligations and enforcement mechanisms, several structural issues persist. These include the broad exemptions provided to government agencies, limited individual rights, the absence of an independent regulatory authority and uncertainties surrounding cross-border data flows.[29] Such gaps raise

[25] Digital Personal Data Protection Act, 2023, §§ 19–21.
[26] GDPR, arts. 45–49 (Cross-Border Data Transfer Mechanisms).
[27] Digital Personal Data Protection Act, 2023, § 16.
[28] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[29] See Digital Personal Data Protection Act, 2023, §§ 12, 16, 17, 19–21.

concerns regarding whether the Act adequately safeguards informational autonomy in a rapidly expanding digital environment.

In an era where personal data fuels economic systems, governance models and digital public infrastructure, the need for a robust and rights-respecting data-protection framework is more urgent than ever. Strengthening the DPDPA through clearer safeguards, greater institutional independence and enhanced individual rights would not only align India with global standards but also ensure that constitutional values remain central to technological transformation.

Ultimately, the future of India's digital governance depends on striking a careful balance between innovation, administrative efficiency and the fundamental right to privacy. A rights-centric approach anchored in constitutional doctrine and supported by transparent regulatory oversight will be essential for ensuring a secure, trustworthy and democratic data ecosystem.