International Journal of Professional Development
Vol.14, No.2, July-Dec. 2025 ISSN: 2277-517X (Print), 2279-0659 (Online)

Data Protection and Informational Privacy Under the Indian Constitution

Dr Arvind kumar
Assistant professor (Resource Person), Department of law
Indira Gandhi University Meerpur, Rewari (Haryana)
Mail id -arvindyadav2712@gmail.com

Abstract
The right to informational privacy and data protection has emerged as one of the most consequential constitutional questions in contemporary Indian jurisprudence. With the Supreme Court of India's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) firmly establishing the right to privacy as a fundamental right under Article 21 of the Constitution, the legal landscape governing personal data has undergone a paradigm shift. This paper undertakes a comprehensive analysis of the constitutional foundations of data protection in India, tracing the evolution of privacy jurisprudence from M.P. Sharma (1954) to the Digital Personal Data Protection Act, 2023. It examines how constitutional values of dignity, autonomy, and liberty converge to shape the framework for informational self-determination, analyses the tensions between state surveillance and individual freedoms, and critically evaluates whether existing legislative mechanisms adequately fulfil the constitutional mandate. The paper argues that while the Puttaswamy judgment laid a robust normative foundation, effective protection of informational privacy demands a constitutionally compliant data governance architecture that centres the individual rather than the state.

Keywords: *Right to Privacy, Article 21, Informational Privacy, Data Protection, Puttaswamy, DPDPA 2023, Fundamental Rights, Surveillance, Autonomy*

Introduction

The digital revolution has fundamentally reordered the relationship between the individual and the state. Every click, transaction, and communication generates data trails that can be aggregated, analysed, and weaponised in ways that the framers of the Indian Constitution could not have anticipated. The constitutional promise of life and personal liberty under Article 21 — long read expansively by the Supreme Court — faces its most sophisticated modern test in the domain of digital privacy and data protection.

India is home to the world's largest biometric identity database (Aadhaar), operates one of the fastest-growing internet ecosystems, and has recently enacted the Digital Personal Data Protection Act, 2023 (DPDPA). Yet the adequacy of these structures when measured against constitutional guarantees remains a subject of intense legal and academic debate. The constitutional right to privacy, though now authoritatively settled, must be operationalised through statutory frameworks that respect the limitations imposed by proportionality, necessity, and accountability.

This paper proceeds in five parts. It begins by charting the historical trajectory of privacy jurisprudence in India before the Puttaswamy judgment, then examines the constitutional foundations articulated in that landmark case. It subsequently analyses informational privacy as a distinct dimension of the right to privacy, evaluates the legislative framework including the DPDPA 2023, and concludes with an assessment of the gaps and reforms necessary to honour the constitutional mandate.

Historical Evolution of Privacy Jurisprudence in India

The Pre-Puttaswamy Era

For over six decades following the Constitution's commencement in 1950, the existence of a

freestanding fundamental right to privacy in India remained constitutionally uncertain. The Supreme Court's early pronouncements were sceptical. In M.P. Sharma v. Satish Chandra (1954), an eight-judge bench held that the Indian Constitution did not guarantee a right to privacy akin to the Fourth Amendment of the United States Constitution, a position reinforced in Kharak Singh v. State of Uttar Pradesh (1962), where a six-judge bench denied the existence of a constitutional right to privacy, though individual justices dissented.

A gradual judicial recalibration began with Gobind v. State of Madhya Pradesh (1975), where Justice Mathew recognised a limited right to privacy derived from Articles 19 and 21, subject to compelling state interest. Subsequent decisions in R. Rajagopal v. State of Tamil Nadu (1994), People's Union for Civil Liberties v. Union of India (1997), and Selvi v. State of Karnataka (2010) progressively affirmed specific aspects of privacy — including informational privacy and the right against testimonial compulsion — without conclusively resolving the foundational question.

The launching of Aadhaar and the consequent petitions challenging mandatory biometric enrolment brought the question to a decisive head. The government's stance, that no fundamental right to privacy existed in Indian constitutional law, made a nine-judge bench reference inevitable.

2.2 The Puttaswamy Judgment (2017): A Constitutional Watershed

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, rendered by a nine-judge Constitution Bench, unanimously overruled M.P. Sharma and Kharak Singh and held that the right to privacy is a fundamental right intrinsic to Articles 14, 19, and 21 of the Constitution. The six separate concurring opinions, while agreeing on the core holding, articulated rich and diverse philosophical foundations for the right.

Justice D.Y. Chandrachud, writing for himself and three other justices, grounded privacy in human dignity, locating the right as a precondition for the exercise of all other liberties. He explicitly recognised informational privacy as a component, stating that individuals must retain control over their personal data and that the state's collection and use of such data must be governed by a legal framework consistent with constitutional values. Justice Kaul, in a separate opinion, emphasised the horizontal application of the right, acknowledging that private actors — corporations and platforms — equally implicate privacy interests, a crucial recognition in the context of big data capitalism.

The judgment established that any limitation on the right to privacy must satisfy a three-part test: (i) legality — the restriction must be sanctioned by law; (ii) legitimate aim — it must pursue a valid state objective; and (iii) proportionality — the means must be proportionate to the ends and represent the least restrictive option available. This framework became the constitutional template against which all subsequent data governance measures must be assessed.

Informational Privacy as a Constitutional Right

Conceptual Contours

Informational privacy, or the right to informational self-determination — a concept developed by the German Federal Constitutional Court in its landmark Census Case (1983) — refers to the individual's right to decide what personal data is collected, how it is used, and with whom it is shared. The Supreme Court in Puttaswamy expressly adopted this conception within the Indian constitutional framework, acknowledging that personal data is an extension of individual personhood and that its misuse threatens not merely personal interests but democratic governance itself.

The philosophical roots of informational privacy connect intimately to the constitutionally protected values of dignity (recognised in the Preamble and Article 21), autonomy (implicit in the freedoms under Articles 19 and 21), and liberty. A person who cannot control information about themselves cannot fully exercise agency over their life — their professional choices, associations, beliefs, and relationships all become

subject to external surveillance, chilling self-expression and dissent.

Dimensions of Informational Privacy

The right to informational privacy encompasses several distinct but overlapping interests. First is the right against unauthorised collection: individuals should not have their personal information gathered without free, informed, and specific consent. Second is the right against unlawful retention: data should not be stored beyond the purpose for which it was collected, a concept expressed in data minimisation and purpose limitation principles. Third is the right against non-consensual disclosure: sharing personal data with third parties without consent or legal basis constitutes a constitutional violation.

Fourth, and critically in the Indian context, is the right against state surveillance. The existence of mass surveillance programmes — whether through NATGRID (National Intelligence Grid), the Central Monitoring System (CMS), or Aadhaar-linked databases — raises profound constitutional concerns about chilling effects on speech and association, discriminatory profiling, and the systematic erosion of anonymity in public and private spheres. The Supreme Court in Anuradha Bhasin v. Union of India (2020) and Faheema Shirin v. State of Kerala (2019) further reinforced that internet access and digital freedoms fall within the constitutional canopy.

The Legislative Framework for Data Protection

Pre-DPDPA Landscape

Prior to the enactment of a comprehensive data protection statute, India's legal framework for personal data was fragmented and inadequate. Section 43A of the Information Technology Act, 2000 (as amended in 2008) imposed liability on body corporates for negligent handling of sensitive personal data, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provided a rudimentary regime applicable only to commercial entities. These instruments fell far short of constitutional requirements: they did not bind government agencies, lacked an independent supervisory authority, and contained no meaningful rights for data principals.

The Justice B.N. Srikrishna Committee, constituted in 2017 in the wake of the Puttaswamy judgment, produced a detailed report in 2018 accompanied by a draft Personal Data Protection Bill. The Committee's report drew on comparative frameworks — the European Union's General Data Protection Regulation (GDPR) in particular — and recommended a rights-centric model with obligations on both private fiduciaries and the state. Subsequent iterations of the bill went through multiple revisions; the 2019 version introduced the controversial non-personal data framework and was eventually withdrawn in 2022.

The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) received presidential assent on 11 August 2023 and represents India's first comprehensive statutory framework for the protection of personal data. The Act applies to the processing of digital personal data within India, as well as processing outside India if it involves offering goods or services to data principals in India — a jurisdictional formulation mirroring GDPR's extraterritorial reach.

The Act introduces several notable provisions: it requires Data Fiduciaries (entities processing data) to obtain free, informed, specific, unconditional, and unambiguous consent before processing personal data, subject to legitimate uses enumerated in the statute. Data Principals (individuals) are granted rights to access information, correct inaccurate data, erasure, grievance redressal, and nomination. The Act establishes a Data Protection Board of India as the adjudicatory body, and prescribes significant financial penalties for contraventions, with maximum penalties reaching INR 250 crore for certain breaches.

However, critical concerns have been raised about the Act's constitutional compatibility. The most significant is the breadth of exemptions granted to the Government of India under Section 17, which permits the central government to exempt any instrumentality of the state from the Act's

provisions — a carve-out so wide that it effectively places the state's data processing activities beyond the reach of the data protection regime. This sits uneasily with the Puttaswamy requirement that restrictions on privacy be proportionate and operate pursuant to a specific legal framework rather than blanket executive discretion.

Constitutional Assessment of the DPDPA

Evaluated against the Puttaswamy proportionality test, the DPDPA presents a mixed picture. On the positive side, the consent-based architecture, purpose limitation requirements, and individual rights broadly accord with constitutional values of autonomy and dignity. The extraterritorial application reflects an understanding that constitutional rights must be effective in the digital age.

On the negative side, the governmental exemptions represent the most constitutionally vulnerable aspect. The Supreme Court in Puttaswamy explicitly cautioned that the state cannot claim a general licence to intrude on privacy for ill-defined national security reasons; any restriction must be proportionate and specific. A blanket exemption allowing the executive to opt out of data protection obligations fails this test. Additionally, the absence of an independent oversight mechanism — the Data Protection Board is not constitutionally insulated from executive influence — raises concerns about whether enforcement will be robust when government agencies are the violators.

5. State Surveillance, Aadhaar, and Constitutional Limits

The Aadhaar ecosystem represents perhaps the most contested intersection of data protection and constitutional rights in India. In Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar case) (2018) 1 SCC 809, a five-judge Constitution Bench — by a 4:1 majority — upheld the constitutional validity of the Aadhaar Act, 2016, while striking down certain provisions and circumscribing mandatory linkage to private services. The majority held that Aadhaar's architecture, with its authentication logs, biometric data, and UIDAI database, did not constitute a surveillance apparatus, given the existing statutory protections.

The lone dissent by Justice D.Y. Chandrachud, subsequently elevated to Chief Justice, is widely regarded as more constitutionally sound. He characterised the Aadhaar architecture as enabling a surveillance state, capable of constructing detailed profiles of citizens through seeding of the Aadhaar number across multiple databases. He held that the Act violated the right to privacy and struck at the foundations of a democratic society premised on individual dignity. His dissent anticipates the growing use of algorithmic governance and predictive surveillance that has intensified in subsequent years.

The constitutional limits on state surveillance remain underarticulated in Indian law. The interception of communications under Section 5 of the Indian Telegraph Act, 1885 and Section 69 of the IT Act are subject to procedural conditions but no independent judicial oversight — a deficiency that stands in stark contrast to comparative constitutional orders. The United States Foreign Intelligence Surveillance Court, the United Kingdom's Investigatory Powers Tribunal, and the European Court of Human Rights standards all require some form of independent authorisation before mass surveillance is constitutionally permissible.

Comparative Constitutional Perspectives

Comparative constitutional analysis illuminates both the promise and the gaps in India's framework. The European Union's approach, anchored in Article 8 of the Charter of Fundamental Rights, treats data protection as a fundamental right distinct from but related to privacy. The GDPR operationalises this right through a comprehensive regime binding both private actors and public authorities equally, enforced by independent supervisory authorities with genuine powers of investigation and sanction.

The German Federal Constitutional Court's development of informational self-determination, the South African Constitutional Court's recognition of privacy under Section 14 of the

Constitution of the Republic of South Africa, 1996, and the Inter-American Court of Human Rights' jurisprudence on digital privacy all suggest a global convergence toward treating informational privacy as a non-derogable constitutional interest, subject only to narrowly tailored limitations proportionate to legitimate state aims.

India's jurisprudential trajectory largely aligns with this global trend, and the Puttaswamy judgment is internationally recognised as a landmark contribution to privacy law. The challenge lies in the implementation gap — the distance between constitutional promise and statutory reality.

Conclusion

The constitutional architecture for data protection and informational privacy in India has been substantially constructed by the Supreme Court in Puttaswamy, but remains only partially realised in statutory form. The right to informational privacy is now firmly embedded in Article 21, demanding that any governmental or private processing of personal data satisfy the tripartite test of legality, legitimate aim, and proportionality. The DPDPA 2023 represents meaningful progress toward a statutory framework consonant with these constitutional requirements, but its broad governmental exemptions, the absence of an adequately independent oversight body, and the dilution of the consent framework in certain provisions render it constitutionally vulnerable.

Three reforms are essential for the realisation of the constitutional mandate. First, the governmental exemptions under Section 17 of the DPDPA must be narrowed to specific, enumerated circumstances subject to independent judicial oversight, not open-ended executive discretion. Second, the Data Protection Board must be insulated from executive control, whether through constitutional provision or robust statutory protection of its members' tenure and independence. Third, India urgently requires a surveillance reform law that establishes judicial authorisation requirements, sunset clauses, and transparency obligations for state interception and data collection programmes.

Ultimately, informational privacy is not merely a technical legal question but a democratic imperative. In a constitutional republic premised on individual dignity and the rule of law, citizens must retain meaningful control over their digital personhood. The Indian Constitution, interpreted through the prism of Puttaswamy, supplies the normative foundation for this control. The task for legislators, regulators, and courts in the coming decade is to build an edifice worthy of that foundation.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Nine-Judge Bench).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2018) 1 SCC 809 (Five-Judge Bench).
3. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (Eight-Judge Bench).
4. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (Six-Judge Bench).
5. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
6. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
7. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
8. Selvi v. State of Karnataka, (2010) 7 SCC 263.
9. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
10. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
11. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
12. Information Technology Act, 2000 (as amended in 2008).
13. Bhatia, G. (2019). The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India.
14. Srikrishna Committee Report: A Free and Fair Digital Economy — Protecting Privacy, Empowering Indians (2018). Ministry of Electronics and Information Technology, Government of India.

15. Chinmayi Arun, 'Privacy in the Age of Aadhaar' (2018) 3 Indian Law Review 1.
16. Shyam Divan & Arghya Sengupta, 'Informational Privacy and the Constitution' (2018) Economic & Political Weekly.
17. Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the European Union, L 119/1.
18. Volkszahlungsurteil [Census Act Case], BVerfGE 65, 1 (1983), German Federal Constitutional Court.
19. Rohan George, 'Data Protection in India: From Puttaswamy to the DPDPA' (2023) National Law School of India Review 88.
20. Vrinda Bhandari, 'The Surveillance State and Article 21: Constitutional Limits on Interception in India' (2022) 14 NUJS Law Review 45.