

Privacy And Data Protection: The Emerging Ambit of Fundamental Rights in India

Bhumika Sidana

Faculty of Law, Tanta University

doi.org/10.64643/IJIRTV12I6-191358-459

Abstract—The concepts of privacy and data protection have emerged as fundamental rights necessary for maintaining and protecting human dignity and autonomy in today's digital world. It was the Right to Privacy that was held by the Supreme Court of India, in the landmark decision of Justice K.S. Puttaswamy v. Union of India¹, to be a Fundamental Right under Article 21 of the Constitution of India. Such recognition emphasizes that privacy is inherent in life and liberty; it protects decisional autonomy, bodily integrity, and personal information from misuse. In reality, however, the constantly growing digital ecosystem faces serious challenges due to the rapid technological advancement, inadequate mechanisms for enforcement, and interests of competing national security and public welfare.

India's landscape of data protection moved from being sector-specific regulations ingrained in laws like the Information Technology Act, 2000, and its 2011 rules to a more comprehensive framework with the passage of the Digital Personal Data Protection Act, 2023. The DPDP Act emphasizes consent-based processing, rights of data principals, and obligations on data fiduciaries, apart from heavy penalties for violations. Still, there are lacunae in the area of enforcement, general awareness among the public, and cybersecurity infrastructure.

Judicial precedents in case like *R. Rajagopal v. Tamil Nadu*¹³⁸ has strengthened the right to privacy, addressing issues as varied as the unauthorized disclosure of personal information to protection against intrusive surveillance techniques.

It would also be recommended that empowering the Data Protection Board, increasing public education on data rights, enforcing strict accountability for data fiduciaries, adopting robust cybersecurity measures, ensuring efficient grievance redressal, and bringing in harmony in cross-border data transfer rules are done to further strengthen the protection of privacy and data in India. This set of precautions will help in protecting the fundamental rights of citizens in a data-driven world,

ensuring that privacy remains a cornerstone of democratic freedoms and individual autonomy.

The research paper discusses the evolving legal framework, identifies areas of continuing challenge, and suggests the way forward to strengthen privacy and data protection as fundamental rights in India.

Keywords: Privacy, Data Protection, Fundamental Rights, Digital Personal Data Protection Act 2023, Right to Privacy in India.

I. INTRODUCTION

The Indian Constitution is a transformative document built upon the foundational value of human dignity. This commitment finds its strongest articulation in Article 21, whose interpretation has steadily evolved from a narrow guarantee of physical existence to a broad assurance of living with dignity. After *Maneka Gandhi v. Union of India*¹, the Supreme Court adopted a liberal and purposive reading of fundamental rights, holding that personal liberty includes a wide range of facets necessary for individual development.

In the digital era, this understanding of dignity has acquired a new and complex dimension—informational dignity. Individuals today participate in both physical and digital spaces, where personal information is continuously collected, analysed, and often monetised. Digital systems such as Aadhaar-enabled DBT schemes, UPI transactions, telemedicine platforms, and social media ecosystems have enhanced accessibility and convenience. However, they also expose individuals to extensive risks of profiling, behavioural targeting, and State or corporate surveillance.

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*² marked a constitutional

¹ AIR 1978 SC 597

² (2017) 10 SCC 1

turning point by affirming privacy as a fundamental right inherent in Articles 14, 19, and 21. It recognized that autonomy and personal liberty are incomplete without control over one's personal information. Yet, translating judicial recognition into effective legal protection remains challenging. The Digital Personal Data Protection Act, 2023 (DPDP Act), represents India's first comprehensive attempt to regulate personal data, but serious questions remain regarding its sufficiency and alignment with constitutional standards.

This paper examines the evolution of privacy jurisprudence in India, analyses the doctrinal depth of Puttaswamy, and evaluates how far the DPDP Act meets the constitutional expectations of necessity, proportionality, and fairness.

II. THE EVOLUTION OF PRIVACY: PRE-PUTTASWAMY JURISPRUDENCE

A. An Era of Judicial Hesitation

Early constitutional jurisprudence adopted a strict textual approach. In *M.P. Sharma v. Satish Chandra*³, the Court observed that the Framers deliberately omitted an explicit protection of privacy, especially concerning search and seizure. Similarly, in *Kharak Singh v. State of Uttar Pradesh*⁴, the majority rejected privacy as a standalone right, despite striking down intrusive police surveillance practices.

Notably, Justice Subba Rao's dissent in *Kharak Singh* served as a visionary foundation for the future. He asserted that liberty under Article 21 must naturally include privacy, as constant surveillance renders all freedoms illusory.

B. Gradual Judicial Recognition

With the changing socio-legal environment, the Court gradually advanced privacy in a number of landmark decisions:

1. *Gobind v. State of Madhya Pradesh*⁵:

The Court accepted that privacy is implicit in Articles 19 and 21, though subject to reasonable restrictions grounded in compelling State interest.

2. *R. Rajagopal v. State of Tamil Nadu*⁶:

It was popularly known as the "Auto Shankar case." This judgment recognized the "right to be let alone" and laid down the foundation of informational and decisional privacy.

3. *PUCL v. Union of India*⁷:

The Court held that telephone conversations fall within the right to life and personal liberty and as such, strict procedural safeguards against arbitrary surveillance were required.

Despite this progressive recognition, privacy remained fragmented and was not ubiquitously grounded in the Constitution until *Puttaswamy*.

III. THE DOCTRINAL FOUNDATION: JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA⁸

The nine-judge bench decision in *Puttaswamy* elevated privacy to a central constitutional guarantee, declaring it intrinsic to human dignity and liberty.

A. Privacy Within the Constitutional Trinity—Articles 14, 19, and 21

The Court found privacy at the junction of the Golden Triangle:

- Article 21-Life and Liberty: Privacy is necessary to protect autonomy, bodily integrity, and decisional freedom.
- Article 19 (Freedoms): Surveillance creates a chilling effect, deterring individuals from freely exercising speech, movement, and association.
- Article 14: Equality Arbitrary, discriminatory, or automated data processing violates fairness and equal protection.

Thus, privacy is not a singular right but a cluster of protections necessary for democratic citizenship.

B. The Four-Part Proportionality Test

To analyze invasions of privacy, the High Court established a structured test:

1. *Legality*: The intrusion should always be based on valid law.
2. *Legitimate Aim*: The aim should be necessary in a democratic society.

³ AIR 1954 SC 300

⁴ AIR 1963 SC 1295

⁵ (1975) 2 SCC 148

⁶ (1994) 6 SCC 632

⁷ (1997) 1 SCC 301

⁸ (2017) 10 SCC 1

3. *Appropriateness*: The means should be rationally related to the objective.

4. *Necessity & Proportionality*: The State should adopt the least intrusive method available.

This test has since become the constitutional benchmark for evaluating privacy restrictions.

IV. THE LEGISLATIVE RESPONSE: THE DPDP ACT, 2023⁹

A. The IT Act, 2000: Beyond and above

Prior to the DPDP Act, data protection in India was governed primarily by the IT Act, 2000, and the SPDI Rules, 2011¹⁰. These instruments were limited in scope, focusing largely on sensitive personal data and failing to provide a general rights-based regime. The Srikrishna Committee Report (2018)¹¹ underscored the urgent need for comprehensive privacy legislation aligned with global standards.

B. Salient Features of the DPDP Act

The DPDP Act introduces a few critical concepts:

- Data Principal–Data Fiduciary model putting individual agency at its core
- Consent-based processing, requiring consent to be free, informed, specific, and unconditional
- Purpose limitation and data minimization, preventing excessive data collection
- The Data Protection Board of India (DPBI), empowered to adjudicate complaints and impose penalties up to ₹250 crore

While the Act represents a significant step forward, many of its provisions require careful scrutiny.

V. CRITICAL EVALUATION: GAPS BETWEEN PRINCIPLE AND PRACTICE

A. The Category of "Legitimate Uses"

Section 7¹² allows data processing without consent for "legitimate uses." The vague and broad phrasing especially the assumption of voluntary data provision that could lead to overbroad interpretations, weakening the centrality of consent.

B. Section 17 and State Exemptions

Section 17¹³ permits the Central Government to exempt any of its agencies from the Act for reasons such as sovereignty or public order. Unlike global frameworks such as the GDPR, the Act does not mandate judicial, parliamentary, or independent oversight for these exemptions. This raise concerns under the Puttaswamy proportionality standard and opens the possibility of unchecked State surveillance.

C. Issues of DPBI Independence

The DPBI's structural dependence¹⁴ on the Executive particularly regarding appointments, terms of service, and removal weakens its credibility as an independent regulator. Effective enforcement requires a body that can hold both private entities and the State accountable.

D. Limited Individual Rights

The Act also limits important individual rights recognized internationally. It does not provide a full-fledged Right to Data Portability, which would allow individuals to move their personal data across platforms, reducing their control over how their information is used. Similarly, the Right to be Forgotten is only partially recognized, restricting an individual's ability to remove or de-index outdated or harmful data. These omissions weaken the principle of informational self-determination and create a noticeable gap between India's framework and global data protection standards.

VI. REMAINING HURDLES

A. The Consent Paradox

Low digital literacy¹⁵ makes consent forms difficult to comprehend, turning consent into a symbolic rather than meaningful act. Stronger standards for notice, transparency, and user-friendly consent mechanisms are necessary to ensure informed decision-making.

B. Cybersecurity Loopholes

Although the Act requires breach reporting to the DPBI, details such as timelines, format, and penalties

⁹ Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

¹⁰ Information Technology Act, 2000, Section 43A; SPDI Rules, 2011.

¹¹ Justice B.N. Srikrishna Committee Report on Data Protection, Govt. of India, 2018

¹² DPDP Act, 2023, Section 7

¹³ DPDP Act, 2023, Section 17

¹⁴ DPDP Act, 2023, Chapter VI (Constitution of DPBI)

¹⁵ National Digital Literacy Mission (NDLM) Report, Ministry of Electronics & IT

are delegated to future rules. Without robust cybersecurity norms and mandatory disclosure mechanisms, India remains vulnerable to significant data breaches.

C. Cross-border Data Transfer¹⁶

The Act adopts a “blacklist” approach, allowing data transfers to all countries except those notified by the Government. While business-friendly, this places an immense burden on the Government to monitor and evaluate international data protection frameworks.

VII. CONCLUSION AND RECOMMENDATIONS

The recognition of privacy as a fundamental right in Puttaswamy marked a milestone in India’s constitutional journey. The DPDP Act, 2023, represents a significant legislative step, but several inconsistencies remain in its ability to meet constitutional thresholds. To align the Act with the values of fairness, autonomy, and proportionality, India must:

1. Establish independent review of State exemptions
2. Empower the DPBI’s independence and transparency
3. Implement an omnibus surveillance reform package
4. Promote digital literacy and privacy awareness

As India transitions into a data-driven economy, protecting *privacy is not merely a legislative responsibility but a constitutional imperative*¹⁷. Ensuring meaningful data rights is essential to safeguard autonomy, dignity, and democratic participation in the digital age.

REFERENCES

Books

- [1] M.P. Jain, *Indian Constitutional Law* (8th edn., LexisNexis, Gurgaon, 2019).
- [2] H.M. Seervai, *Constitutional Law of India* (4th edn., Universal Law Publishing, New Delhi, 2013).
- [3] Durga Das Basu, *Introduction to the Constitution of India* (LexisNexis, New Delhi, 2018).

Articles & Reports

- [4] B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Committee Report, Ministry of Electronics and Information Technology, Government of India, 2018).
- [5] Justice K.S. Puttaswamy (Retd.) v. Union of India — A Constitutional Analysis, *Indian Law Review* (2018).
- [6] Usha Ramanathan, “Aadhaar: From Welfare to Surveillance”, 43 *Economic and Political Weekly* (2014).

Statutes

- [7] The Constitution of India, 1950.
- [8] Information Technology Act, 2000.
- [9] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- [10] Digital Personal Data Protection Act, 2023.

Case Laws

- [1] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
- [2] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
- [3] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
- [4] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
- [5] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
- [6] *People’s Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
- [7] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

International Instruments

- [1] Universal Declaration of Human Rights, 1948.
- [2] International Covenant on Civil and Political Rights, 1966.
- [3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

¹⁶ DPDP Act, 2023, Section 16

¹⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1