The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PROTECTION AND PRIVACY LAWS IN INDIA

Abhipsa Pati

INTRODUCTION

In the third quarter of 2023, India's wireless data consumption stood at 47,629 petabytes, averaging 15.88 billion gigabytes per month[1], and climbed further in 2024, with TRAI reporting an average of 27.5 GB per user per month[2]. 5G users alone consumed 3.6 times more data than 4G users[3], reflecting not just technological adoption but also the scale at which Indians generate and share personal data. Yet a 2024 PwC India survey[4] found that 56% of citizens remain unaware of their personal data rights, 69% do not know they can withdraw consent, and 87% believe their data is already compromised or publicly accessible.

This disquieting asymmetry between data creation and control raises the question: can India's constitutional and legislative safeguards keep pace with its data economy? The *Justice K.S. Puttaswamy (Retd.) v. Union of India*[5] (2017) judgment declared privacy a fundamental right, and the Digital Personal Data Protection (DPDP) Act, 2023, India's first comprehensive privacy law, sought to give it shape. Yet, as Justice Nariman cautioned, "Fundamental rights… are contained in the Constitution so that there would be rights that the citizens of this country

[1] Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators: July–September 2023, at 30–31 (2024), <https://www.trai.gov.in/sites/default/files/2024-08/PR_No.05of2024.pdf> (last visited July 8, 2025).
[2] Telecom Regulatory Authority of India, Highlights of Telecom Subscription Data as on 31st March, 2024 (2024), <https://www.trai.gov.in/sites/default/files/2024-08/PR_No.31of2024.pdf> (last visited July 8, 2025).
[3] 5G users in India consume 3.6x more data compared to 4G users: Nokia MBiT report, ECONOMIC TIMES (Mar. 20, 2024), <https://economictimes.indiatimes.com/industry/telecom/telecom-news/5g-users-in-india-consume-3-6x-more-data-compared-to-4g-users-nokia-mbit-report/articleshow/108653658.cms> (last visited July 8, 2025).
[4] Consumers worried about data breaches, says PwC India survey, Economic Times (Apr. 2, 2024), <https://economictimes.indiatimes.com/news/company/corporate-trends/consumers-worried-about-data-breaches-says-pwc-india-survey/articleshow/114463457.cms?from=mdr> (last visited July 9, 2025).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

may enjoy despite the governments that they may elect." Today, privacy in India still stands at risk of being eroded by institutional frailty and sweeping state power, as this blog, argues.

FROM CONSTITUTIONAL RECOGNITION TO LEGISLATIVE CODIFICATION

For decades, privacy jurisprudence in India was impoverished. The Supreme Court in *M.P. Sharma v. Satish Chandra*[6] (1954) and *Kharak Singh v. State of Uttar Pradesh*[7] (1962) denied the existence of any constitutional right to privacy. It was *Puttaswamy* in 2017 that marked a decisive turn. In his opinion, Justice D.Y. Chandrachud described privacy as "the constitutional core of human dignity," and "intrinsic to life, liberty, freedom and dignity, and therefore, an inalienable natural right." The judgment conceptualized privacy as both individual and societal. As Justice Chandrachud wrote, "It must be realised that it is the right to question, the right to scrutinize and the right to dissent which enables an informed citizenry to scrutinize the actions of government." Recognizing informational privacy in a data-driven age, the Court imposed a positive obligation on the state to enact legislation ensuring necessity, legality, and proportionality in data collection and use.

THE DPDP ACT, 2023

Until 2023, India's framework for data protection consisted of the IT Act, 2000, and the SPDI Rules, 2011, both inadequate for an era of ubiquitous digital profiling and mass surveillance. The DPDP Act was intended as a corrective, introducing individual rights to access and correct data, withdraw consent, and seek grievance redressal. Data fiduciaries are obligated to limit collection, secure data, and delete it when no longer necessary. Penalties now reach ₹250 crore, and draft rules issued in January 2025 add further obligations: breach notifications within 72 hours, automatic deletion of dormant data after three years, and enhanced safeguards for children's data.

But the Act's normative deficits are glaring. The Data Protection Board is constituted and controlled by the executive, undermining its independence. As Bruce Schneier cautions, "Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect", yet the DPDP grants the state sweeping exemptions for ill-defined grounds of "national security" and "public order." Such carte blanche exemptions, unmoored from judicial scrutiny, threaten to hollow out the very right they purport to regulate. Worse still, the Act ignores the elephant in the room: mass surveillance. As Shoshana Zuboff[8] warns, "Democracy and surveillance capitalism cannot coexist peacefully; one will eventually

[6] M.P. Sharma v. Satish Chandra, 1954 SCR 1077.
[7] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[8] Shoshana Zuboff, The Age of Surveillance Capitalism 11 (PublicAffairs 2019).

supplant the other." India's own Central Monitoring System and other surveillance programs remain outside the Act's ambit, undermining the *Puttaswamy* vision of proportionality and accountability.

These shortcomings matter not just in theory but in practice. The average cost of a data breach in India climbed to ₹19.5 crore[9] in 2024, yet public confidence in institutional safeguards remains low: 82% of consumers now rank data protection as essential to brand trust, while 42% express reluctance to continue with a service after a breach.

TOWARD A CONSTITUTIONALLY FAITHFUL REGIME

For India to realize the promise of *Puttaswamy*, reform must proceed on three fronts. The state's sweeping exemptions must be narrowly tailored, subject to judicial review under the proportionality doctrine. The Data Protection Board must be restructured to operate as an independent and professionally competent authority. Finally, public awareness campaigns are essential, because, as Professor Daniel Solove reminds us, "Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly."

Mass surveillance requires particular scrutiny. Helen Nissenbaum's insight that privacy is "about the appropriate flow of information", should guide reforms to ensure that state power respects contextual integrity rather than exploiting informational asymmetries.

As Chief Justice Misra observed, "I am what I am. So take me as I am. No one can escape from their individuality." Privacy must protect this individuality against both corporate commodification and state overreach.

CONCLUSION

Privacy is not a luxury of the few but the safeguard of dignity, autonomy, and democratic legitimacy. As Justice Sapre aptly noted, privacy "is indeed inseparable and inalienable from [the] human being." The DPDP Act is a long-awaited legislative milestone, but its normative and institutional flaws risk reducing privacy to a nominal right, vulnerable to the very surveillance and arbitrariness it was meant to guard against. Justice Brandeis warned over a century ago that privacy is "the right to be let alone, the most comprehensive of rights and the right most valued by civilized men." That warning resonates more urgently than ever in India's data-driven polity. If privacy is to remain "the constitutional core of human dignity," as Justice Chandrachud called it, then India must act to ensure that the right to privacy is not only recognized but meaningfully realized. The integrity of its democracy depends on it.

---

[9] IBM Security, Cost of a Data Breach Report 2024, at 18 (2024), <https://www.ibm.com/reports/data-breach> (last visited July 10, 2025).