THE RIGHT TO DIGITAL PRIVACY VS. STATE SURVEILLANCE: RETHINKING INDIA'S CONSTITUTIONAL FRAMEWORK AFTER THE DPDP ACT, 2023

Diksha*

ABSTRACT

The constitutional right to privacy, solemnly recognised by the Supreme Court of India in K.S. Puttaswamy v Union of India (2017), has been subjected to its most severe legislative stress test through the Digital Personal Data Protection Act, 2023 (DPDP Act) and the subsequent 2026 amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. As India navigated the dual imperatives of national security and individual liberty, this article examines whether the current statutory framework, particularly the DPDP Act's broad exemptions in favour of state surveillance, satisfies the proportionality standard mandated by Puttaswamy. Drawing on the theory of informational self-determination, comparative analysis of the European Union's General Data Protection Regulation (GDPR), and the evolving discourse around AI-powered surveillance, the article argues that India stands at a constitutional crossroads. The DPDP Act, while symbolically acknowledging privacy as a right, structurally enables an expansive surveillance architecture that is disproportionate, opaque, and constitutionally suspect. A reformed legal framework, grounded in necessity and proportionality, is both urgently needed and constitutionally required.

Keywords: Digital Personal Data Protection Act 2023, Right to Privacy, State Surveillance, Puttaswamy, Proportionality, GDPR, IT Rules 2021, AI Surveillance, Informational Self-Determination, Article 21.

INTRODUCTION: PRIVACY IN THE AGE OF THE ALGORITHMIC STATE

In August 2017, nine judges of the Supreme Court of India unanimously declared that the right to privacy is a fundamental right under the Constitution of India. Justice D.Y. Chandrachud,

*BA LLB, THIRD YEAR, GITARATTAN INTERNATIONAL BUSINESS SCHOOL.

writing for himself and three others, described privacy as a constitutional guarantee against the arbitrary use of state power. The Puttaswamy judgment was celebrated as a constitutional landmark, a definitive rejection of the colonial-era view that citizens had no right against state intrusion into their personal lives. Six years later, Parliament enacted the Digital Personal Data Protection Act 2023, India's first comprehensive data protection legislation. On its face, the DPDP Act appeared to be the legislative fulfilment of Puttaswamy's promise. It established rights of access, correction, and erasure for data principals. It imposed obligations on data fiduciaries. It created the Data Protection Board as a grievance redress mechanism. And then, tucked into Section 17, it carved out sweeping exemptions exempting the State from virtually every protection the Act had just conferred.

By early 2026, the picture had become even more complex. The India-AI Summit 2026 and the simultaneous amendment to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 signalled an active government intent to shape the digital information environment with significant implications for online speech, platform accountability, and the surveillance apparatus that underpins enforcement. This article examines whether the constitutional guarantee of privacy, as articulated in Puttaswamy, survives the legislative choices made in the DPDP Act and the 2026 IT Rules Amendment.

THE PUTTASWAMY PROPORTIONALITY STANDARD: A CONSTITUTIONAL BENCHMARK

The Puttaswamy judgment did not merely recognise privacy as a right; it prescribed the conditions under which the State could legitimately restrict it. Justice Chandrachud's plurality opinion articulated a three-part test: any limitation on privacy must (i) be sanctioned by law; (ii) serve a legitimate state aim; and (iii) be proportionate, meaning it must be the least restrictive measure capable of achieving that aim. This proportionality standard is the constitutional yardstick against which all subsequent data protection and surveillance legislation must be measured. The proportionality doctrine is not merely procedural; it is substantive. A law that authorises mass surveillance of citizens without individualised suspicion, even if it serves a legitimate national security objective, may still fail the proportionality test if its reach is broader than necessary. This is the central tension that the DPDP Act has failed to resolve.

Justice S.K. Kaul, in a concurring opinion in Puttaswamy, went further, calling for a data protection law that would provide a robust framework governing the collection, storage, use, processing, disclosure, transfer, and protection of personal data. The DPDP Act was Parliament's answer to that call. The question is whether it measures up.

SECTION 17 OF THE DPDP ACT: THE SURVEILLANCE CLAUSE IN PLAIN SIGHT

Section 17 of the Digital Personal Data Protection Act, 2023, is arguably the most consequential provision in the statute and the most constitutionally controversial. It exempts the Central Government and any instrumentality of the State from the application of the Act where processing of data is deemed necessary for (a) security of the State, (b) public order, (c) prevention of offences, or (d) any purpose prescribed by the Central Government through notification.

The breadth of this exemption cannot be overstated. 'Security of the State' and 'public order' are notoriously elastic terms in Indian constitutional law, capable of being stretched to cover a wide range of state activities. The addition of a residual category 'any purpose prescribed by the Central Government' effectively places the outer limit of the exemption in the hands of the executive, without any independent judicial or parliamentary oversight. This structure is constitutionally suspect for at least two reasons. First, it fails the proportionality test articulated in Puttaswamy, a blanket exemption is the antithesis of a 'least restrictive measure.' Second, it creates what constitutional scholars have termed an 'accountability vacuum': state agencies processing personal data under Section 17 are not required to disclose the nature, extent, or purpose of their data processing to the Data Protection Board, to Parliament, or to the affected individuals.

The contrast with the European Union's GDPR is instructive. Article 23 of the GDPR permits member states to restrict certain data subject rights for national security purposes, but only through specific legislative measures that must include clear provisions on the purpose, categories of data, scope of restrictions, safeguards against abuse, and the right to judicial redress. The DPDP Act's Section 17, by contrast, requires none of these safeguards.

AI-POWERED SURVEILLANCE AND THE NEW FRONTIER OF PRIVACY VIOLATIONS

The 2026 amendment to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, enacted in the immediate aftermath of the India-AI Summit 2026, has sharpened the urgency of this analysis. The amendment expanded the compliance obligations of significant social media intermediaries while also strengthening government powers to direct the takedown of content and the identification of originators of messages. Critics have argued that these expanded powers, when combined with AI-based content moderation and surveillance tools, create a digital panopticon that operates in the shadow of the DPDP Act's Section 17 exemptions.

AI-powered surveillance encompassing facial recognition systems at public spaces, social media monitoring tools, predictive policing algorithms, and mass metadata collection programmes poses qualitatively different threats to privacy than traditional surveillance. Its scale is virtually unlimited. Its operation is invisible to the surveilled individual. Its outputs can form the basis of consequential decisions, including law enforcement action, without any human review. The Supreme Court's observation in Puttaswamy that 'the right to privacy is not absolute' is frequently invoked by proponents of state surveillance. But the Puttaswamy court was equally clear that the burden of justification lies with the State, not the citizen. A State that cannot explain the necessity, scope, and oversight mechanisms of its surveillance programmes cannot satisfy Puttaswamy's proportionality requirement, regardless of how broadly Section 17 of the DPDP Act is worded.

INFORMATIONAL SELF-DETERMINATION: THE MISSING RIGHT IN INDIA'S FRAMEWORK

The German Constitutional Court's landmark Volkszahlungsurteil (Census Judgment) of 1983 articulated the concept of informational self-determination, the right of individuals to determine, in principle, when and within what limits information about themselves may be communicated to others. This concept has since become foundational to data protection law across democratic jurisdictions.

Justice Chandrachud's opinion in Puttaswamy appears to embrace informational self-determination as a component of the right to privacy in India, describing privacy as including the ability of the individual to prevent the sharing of information about herself. Yet the DPDP

Act operationalises this right in an attenuated form. The consent mechanism, the Act's primary tool for data principal empowerment, is riddled with exceptions for 'legitimate uses' and 'reasonable purposes' that significantly dilute its practical effect.

More critically, the Act does not recognise a freestanding right to informational self-determination as against the State. There is no equivalent of Article 8 of the EU Charter of Fundamental Rights, which explicitly protects personal data as a distinct fundamental right in India's statutory or constitutional framework. The DPDP Act treats data protection primarily as a regulatory matter, not a rights-based one. This conceptual gap has direct consequences for the enforceability of privacy rights against state surveillance.

TOWARDS A CONSTITUTIONALLY COMPLIANT FRAMEWORK: RECOMMENDATIONS

Reforming India's digital privacy architecture to meet the Puttaswamy standard requires targeted interventions at the legislative, institutional, and judicial levels.

Narrowing Section 17: The blanket state exemption must be replaced with a structured necessity and proportionality test. Any derogation from the DPDP Act's protections for state surveillance purposes should require: (i) a specific statutory authorisation rather than executive notification; (ii) independent judicial or quasi-judicial oversight before data is accessed; (iii) time-limits on data retention; and (iv) mandatory post-facto notification to the affected individual wherever operationally feasible.

Strengthening the Data Protection Board: The Data Protection Board of India, as currently constituted under the DPDP Act, lacks the structural independence necessary to effectively scrutinise state surveillance programmes. The Board's composition, appointment process, and jurisdiction should be reformed to ensure genuine independence from the executive, with explicit jurisdiction to investigate complaints against state data processing, including processing under Section 17.

Judicial Review Mechanism. India should consider a specialised digital rights tribunal or a dedicated bench within the High Courts for adjudicating privacy and data protection disputes, with the power to review surveillance authorisations and grant interim relief. This is consistent with the international trend towards specialised data courts and with the Supreme Court's own observation in Puttaswamy about the need for institutional safeguards.

Algorithmic Transparency Mandate. Any AI-powered surveillance system deployed by the State should be subject to mandatory algorithmic impact assessments, published in an accessible form. Citizens should have the right to know when AI systems have made decisions affecting them and to seek human review of those decisions, a principle embedded in Article 22 of the GDPR that India's framework should adopt.

CONCLUSION

The right to digital privacy is not a luxury of the affluent or the technologically literate. In an era where every online interaction generates data, every movement is potentially tracked, and every communication is potentially monitored, privacy is the precondition for all other freedoms: speech, association, belief, and dissent. The Supreme Court understood this in Puttaswamy. The legislature must understand it in law.

The Digital Personal Data Protection Act 2023 was an opportunity to translate Puttaswamy's constitutional promise into a statutory reality. That opportunity has been partially squandered. Section 17's sweeping exemptions, the weak institutional design of the Data Protection Board, and the absence of a meaningful legal framework for AI surveillance combine to create a digital rights deficit that the Constitution does not permit.

As India continues to expand its AI capabilities and its digital governance infrastructure, the pressure on the privacy guarantee will only intensify. The legal community, through litigation, scholarship, and legislative advocacy, must ensure that the State's digital ambitions remain anchored in constitutional values. Privacy, as Justice Chandrachud wrote, is a guaranteed right of the citizen to be protected against the march of technology. The march has not slowed. The protection must keep pace.

REFERENCES

1. K.S. Puttaswamy (Privacy-9J.) v Union of India, (2017) 10 SCC 1.
2. K.S. Puttaswamy (Aadhaar-5J) v Union of India, (2019) 1 SCC 1.
3. Maneka Gandhi v Union of India, (1978) 1 SCC 248.
4. Digital Personal Data Protection Act 2023 (Act No. 22 of 2023), ss. 4, 6, 8, 12-16, 17.
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended February 2026.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), Articles 5, 22, 23.
7. Regulation (EU) 2024/1689 (EU Artificial Intelligence Act), Arts. 10, 13, 14.
8. EU Charter of Fundamental Rights, Art. 8.
9. Bundesverfassungsgericht (German Federal Constitutional Court), Volkszahlungsurteil, BVerfGE 65, 1 (1983).
10. Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (MeitY, 2018).
11. Vidhi Centre for Legal Policy, 'Analysis of the Digital Personal Data Protection Bill, 2023' (2023).
12. Internet Freedom Foundation, 'Comments on the DPDP Act, 2023' (2023).