International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Privacy vs. Surveillance in the Digital Age: A Critical Study of India's Digital Personal Data Protection Laws

Shivani[1], Dr. Arti[2], Dr. Avon Kumar Vaid[3]

[1]Research Scholar, Desh Bhagat University, Mandi Gobindgarh, Punjab, India

[2]Assistant Professor, Desh Bhagat University, Mandi Gobindgarh, Punjab, India

[3]Principal, Amritsar Law College, Amritsar, Punjab, India

Abstract: ***The accelerated digitization of governance, trade, and communication in India has led to the question of data privacy at the forefront. As the surveillance apparatus is made more advanced, the dilemma between national security and individual privacy worsens. In this paper, India's Digital Personal Data Protection Act, 2023 (DPDPA) is critically analyzed for its role in protecting personal privacy while providing room for state surveillance. The research analyzes the balance or imbalance between individual rights and state power, using legal, technological, and ethical perspectives. It also engages comparative international frameworks to place India's legislative response within wider privacy debates.***

Keywords: Data Protection, Privacy, Surveillance, DPDPA, India, Digital Rights, State Power, GDPR

1. Introduction

The digital revolution has radically transformed the manner in which personal data is collected, processed, stored, and used. Technological progress in fields like artificial intelligence, biometrics, and big data analytics has made governance swifter, services more focused, and business models streamlined. Yet this change has also raised questions around private life and individual privacy, misuse of data, and state espionage. In the Indian context, these issues came into focus legally and politically in the wake of the important Supreme[1] Court judgment in Justice K.S. Puttaswamy v. Union of India (2017), where the Court judicially recognized by a consensus the right to privacy as a constitutional right under Article 21 of the Constitution. The ruling established the platform for an exhaustive data protection regime in India.

In response to the changing data landscape, the Indian Parliament passed the Digital Personal Data Protection Act, 2023 (DPDPA). The Act is India's first standalone law specifically governing digital personal data, defining the rights of the individual (Data Principals) and responsibilities of data handlers (Data Fiduciaries). The Act seeks to give individuals greater control over their data, hold data handlers accountable, and promote digital innovation.

Much as it has progressive motives, the DPDPA has generated widespread controversy. Its critics suggest that the Act vests too much power in the central government, including broad exemptions to state surveillance on grounds of national security. Second, the absence of an autonomous regulatory agency and judicial oversight provisions has raised concerns regarding transparency and accountability.

This essay critically analyzes the DPDPA in the context of the privacy-surveillance divide. It considers whether the bill is a fair balance between protecting personal rights and facilitating essential state surveillance, or whether it potentially leads to the legitimation of a surveillance state for the purposes of national interest and administrative efficiency.

2. Conceptual Framework

2.1 Privacy in the Digital Age

With the emergence of the digital age, privacy went far beyond geographical boundaries. It now extends to informational privacy—a person's capacity to regulate the gathering, use, storage, and sharing of his or her personal information. With the spread of digital technologies, personal information is being continuously produced through web transactions, social networking participation, biometric devices, and mobile programs. Privacy is thus coming to be recognized ever more as the right to informational self-determination: the capacity to determine who accesses one's information, under what circumstances, and for what ends. This realignment is a sign of increasing awareness that control and ownership of data are an inherent component of human autonomy, dignity, and freedom[2] in the 21st century.

2.2 National Security and Surveillance

Surveillance is the systematic monitoring or observation of people, groups, or virtual spaces, usually by state authorities, with the aim of exercising control, ensuring public safety, or maintaining national security. In democratic societies, surveillance is generally justified as a counter-terrorism

[1] Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[2] Freedom House. (2024). Freedom on the Net – India Country Report. https://freedomhouse.org

measure, an aid to law and order, or an early warning system for cyber attacks. Yet, in the absence of effective checks and balances, there is increasingly a blurring between legitimate surveillance and coercive monitoring. When surveillance exercises are undertaken without transparency, proportionality, or judicial control, they can infringe on constitutional rights and facilitate authoritarianism. Therefore, the primary challenge in the digital era is to create legal and ethical frameworks that harmonize surveillance needs with safeguards of privacy for individuals such that national security goals do not supplant constitutional protections.

3. Evolution of Law of Data Protection in India

3.1 Puttaswamy Judgment (2017)

The legal basis for data protection in India was established by the seminal Supreme Court ruling in Justice K.S. Puttaswamy v. Union of India (2017), where a nine-judge constitutional bench unanimously declared that the right to privacy is a fundamental right under Article 21 of the Indian Constitution. The Court acknowledged that in a more digitalized society, privacy must not be limited to personal information and data. It underlined the necessity of a strong legal framework to safeguard individuals from state as well as private interference. The Puttaswamy judgment not only reasserted individual dignity and autonomy but also spurred legislative momentum towards a complete data protection regime in India.

3.2 Development from PDP Bill to DPDPA 2023

Post the Puttaswamy judgment, the Government of India set up a committee headed by Justice B.N. Srikrishna to prepare a data protection framework.

- **2018:** The Srikrishna[3] Committee laid down its report and the draft Personal Data Protection (PDP) Bill, 2018. It suggested a balanced model among data protection and state interests, such as establishing a Data Protection Authority (DPA).
- **2019–2022:** Later drafts of the Bill, such as the Personal Data Protection Bill, 2019, were tabled in Parliament but were criticized for providing sweeping exceptions to the government and weakening the autonomy of the regulatory body. Civil society and lawyers raised alarms on surveillance and insufficient safeguards.
- **2023:** The Digital Personal Data Protection Act, 2023 (DPDPA) was passed, superseding previous drafts. Although it proposed such critical concepts as purpose limitation, consent-based processing, and data fiduciary duties, it also retained controversial elements. These include broad exemptions for the state, softened data localization, and an adjudicatory board under executive authority—questioning its effectiveness in actually safeguarding digital privacy.

[3] Srikrishna Committee. (2018). Report of the Committee of Experts on Data Protection. Ministry of Electronics and Information Technology. https://meity.gov.in

4. Key Provisions of the Digital Personal Data Protection Act, 2023 (DPDPA)

The Digital Personal Data Protection Act, 2023 (DPDPA) is India's first specific legislation for safeguarding individuals' personal data in the digital landscape. In the backdrop of the increasing demand for a regulatory framework on data governance, the Act aims to provide principles of processing of data, delineate roles and responsibilities of stakeholders, and safeguard rights of individuals in a digitally enabled economy. Introducing some progressive provisions, the Act also has certain provisions that have attracted criticism because of apprehensions regarding overreach by the state and lack of institutional autonomy. This section describes and critically examines the most important features of the DPDPA, 2023.

1) Scope and Applicability

The DPDPA covers digital personal data—that is, all personal data in digital form, whether collected online or converted from physical files. Significantly, the Act is extraterritorial in operation, which implies that it also controls the processing of data outside India if it is in relation to providing goods or services to Indian citizens. This clause pulls under its umbrella multinational corporations that process Indian citizens' data so that their processing activities would fall under Indian law. It does not, however, include non-personal data or anonymized data, leaving a void in the general data governance framework.

2) Consent Architecture

Another. foundational aspect of the DPDPA is consent-based processing. The Act requires that personal data be processed only with the express, informed, and voluntary consent of the Data Principal (i.e., the individual whose data is being processed). The request for consent must be explicitly stating the purpose of data processing and must be provided in all 22 languages contained in the Eighth Schedule to the Indian Constitution. This facilitates greater accessibility.

Exceptions exist. Some "legitimate uses" permit non-consensual processing of data—e.g., where employment, legal duty, or medical need is concerned. This gives scope for real-world situations while creating concerns with abuse potential, especially when the "legitimate use" definition is too loose and imprecise.

3) Data Fiduciaries and Data Principals

The Act makes two fundamental concepts: Data Fiduciaries and Data Principals. Data Fiduciaries are organizations—government, private companies, or startups—deciding the purpose and method of processing personal data. Data Principals are people whose data is being processed.

The Act prescribes some rights for Data Principals, such as:

- The right to information regarding processing of their data,
- The right to correction and deletion of personal data,
- The right to redressal of grievances.

Nonetheless, these rights are not unqualified and are qualified by conditions prescribed in the law. The critics suggest that the realization of these rights is watered down by the absence of a solid, independent enforcement system.

4) Exemptions for the State

The most controversial point of the DPDPA is the expansive exemptions to the state in Section 17. The central government can exempt any government organization from the provisions of the Act in the interest of sovereignty, national security, public order, or friendly relations with foreign states.

The exemptions are undesirable for a number of reasons:

- They are not subject to procedural protections and do not have prior judicial or independent sanction.
- There is no duty to notify Data Principals when their data is processed under such exceptions.
- The standards for defining what "national interest" or "public order" are undefined and subject to executive discretion.

This is a source of concern regarding the possibility of untrammelled surveillance and degradation of people's privacy rights.

5) Data Protection Board of India

The Act creates the Data Protection Board of India (DPBI) as the tribunal or adjudicatory organization that will enforce the DPDPA provisions. The Board has the mandate to settle disputes, impose fines, and ensure compliance by Data Fiduciaries.

Yet, the independence of the DPBI is doubtful. The members of the Board, including the Chairperson, are appointed by the central government, which also holds the authority to remove them. The absence of measures that provide protection from interference by the executive seriously detracts from the Board's role as an independent regulator, especially in matters involving state institutions.

Further, the Board does not have suo motu powers and functions mostly on the basis of complaints or references to it, restricting its proactive regulatory role.

6) Cross-Border Data Transfer

The DPDPA takes a comparatively liberal approach to cross-border data transfers. Contrary to previous drafts, which focused on draconian data localization, the 2023 Act allows for personal data to be transferred to nations that the central government might notify from time to time.

This business-oriented approach is conducive to international data flows necessary for cross-border digital services. Yet the absence of transparency regarding how the list of approved countries will be decided raises concerns over the sufficiency of privacy safeguards in the receiving jurisdictions. Absence of clear criteria or public consultation poses a risk to the security of Indian users' data in cross-border data transfers.

7) Penalties and Compliance

In order to hold the corporate entities accountable, the Act levies financial penalties for default, ranging from ₹10,000 to ₹250 crore depending on the nature of the default. Illustratively:

- Insufficient security controls to protect against breaches may entail a penalty of up to ₹250 crore.
- Default in data handling duties for children's data can invite penalties of up to ₹200 crore.

Although these sanctions look harsh, their deterrent value will also rely on the strength of enforcement, which is doubtful with the current limitation of the Data Protection Board.

The Act also contains provisions for voluntary agreements, where firms can commit to taking remedial actions without conceding liability, and thereby lowering their penalties. While this promotes compliance, it should also be watched to avoid abuse or lax enforcement.

5. Critical Analysis: Privacy vs. Surveillance

The Digital Personal Data Protection Act, 2023 (DPDPA) is a pathbreaking effort towards the regulation of personal data in India's rapidly developing digital environment. Although the legislation has some positive provisions in relation to data processing and individual rights, the Act also raises important concerns related to unbridled surveillance, executive overreach, and insufficient institutional protections. A close examination of the DPDPA shows that, instead of balancing privacy and state surveillance, the law could end up weighing heavily in favor of the state, even to the detriment of essential rights.

5.1 Ambiguity in State Exemptions

One of the most controversial aspects of the DPDPA is in Section 17, which gives the central government the authority to exempt any of its agencies or departments from the provisions of the Act in the interests of sovereignty, public order, or national security. Although exemptions in data protection legislation around the world are not uncommon, what's different here is that it has no procedural safeguards. No judicial or parliamentary review is necessary prior to the issuing of such exemptions. This implies that government surveillance can be carried out without notification to the Data Principal and without needing to justify the reasons for so doing in the courts of law. This lack of scrutiny seriously erodes the foundations of accountability, transparency, and proportionality in data regulation.

5.2 Weakening of the Data Protection Authority

The India Data Protection Board, the adjudicatory and enforcement agency under the Act, lacks institutional independence. In contrast to the EU's General Data Protection Regulation (GDPR), which requires independent supervisory authorities, the DPDPA places the central government with the power to appoint and remove members of the Board. This executive direct control gives rise to severe concerns regarding conflicts of interest, particularly when the Board must adjudicate on conflicts between

government agencies. A regulator that is institutionally subject to the executive cannot reasonably be expected to enforce data protection standards impartially, particularly in state surveillance cases.

5.3 Lack of Data Localization

Prior iterations of India's data protection legislation, specifically the 2019 PDP Bill, had also set forth stringent data localization standards, requiring storage and processing of certain types of sensitive personal data within India. The DPDPA 2023, however, eases these requirements considerably, enabling personal data to be outsourced to countries that are recognized by the central government. While this is useful for multinational companies and lessens regulatory obstacles, it does increase the risk of foreign monitoring and abuse of data. In the absence of robust localization standards or protections covering transfers across the border, Indian citizens' personal data can be at risk of being accessed by foreign governments or intelligence agencies.

5.4 Opaque Surveillance Infrastructure

India's surveillance framework is already widespread, with the Central Monitoring System (CMS), National Intelligence Grid (NATGRID), and Crime and Criminal Tracking Network and Systems (CCTNS) all running with limited public scrutiny. These frameworks allow for central, real-time monitoring of communication and activities on multiple platforms. However, they run without a complete legal framework and independent monitoring frameworks. The DPDPA does not cover or control the existing surveillance infrastructure, nor does it require transparency or public disclosure. Its absence not only legitimates secret surveillance but also does not include India's overall surveillance practices within a framework of rights.

5.5 Comparison with International Standards

In comparison to international data protection frameworks like the European Union's General Data Protection Regulation (GDPR), the DPDPA is inadequate in some critical respects. The GDPR curbs state surveillance rigorously and demands independent judicial or parliamentary consent in the case of exceptions. It enshrines strong individual rights like the right to be forgotten, the right to data portability, and the right to explanation in automated decision-making. It also requires frequent audits and imposes accountability through independent supervisory institutions. As opposed to the DPDPA, it provides minimal user rights and emphasizes executive discretion over autonomy. The lack of an independent regulator of data and inadequate binding state obligations for the latter demonstrates a surveillance-laden strategy under the pretext of data protection.

6. Implications for Democratic Governance

The passage of the Digital Personal Data Protection Act, 2023, in its present shape has long-reaching consequences for democratic democracy in India, especially in the context of basic rights, institutional accountability, and public faith.

Chilling Effect on Free Speech

Extravagant surveillance powers accorded to the state, particularly in the absence of advance judicial intervention, can have a chilling effect on free speech. Citizens are likely to be cautious to express dissenting views or engage in politically sensitive talks for fear of being watched over by their digital record. Self-censorship undermines democratic debate and erodes the fundamental right to freedom of speech under Article 19 of the Constitution.

Surveillance regimes without openness and accountability tend to disproportionately target vulnerable groups, such as minorities, political activists, journalists, and human rights defenders. The lack of protective measures within the DPDPA to avoid targeted surveillance raises questions about discriminatory behavior and the use of personal data for profiling or silencing vulnerable groups.

Erosion of Public Trust

Generalised fears regarding state monitoring can undermine public faith in digital public infrastructure like Aadhaar, DigiLocker, and other elements of IndiaStack. Citizens might delay taking advantage of digital offerings lest their private information be viewed or manipulated by the government without permission. Such distrust undermines the purpose of digital inclusion and derails the success of e-governance initiatives.

In conclusion, while it is in order to be concerned with national security, any spy systems must be proportionate, transparent, and open to independent review. To fail to observe these safeguards does not just infringe on individual privacy but actually threatens the very health of India's democratic institutions.

7. Recommendations

To ensure that the Digital Personal Data Protection Act, 2023 (DPDPA) truly upholds the right to privacy and prevents the misuse of state surveillance powers, a series of structural and legal reforms are essential:

1) **Judicial Oversight:** Implement an automatic mechanism mandating prior judicial approval for government agencies' access to all surveillance-related data. This would guarantee that surveillance is based on a reasonable justification, proportionate, and accountable under the constitution to prevent arbitrary encroachment on personal privacy.
2) **Independent Data Authority:** Redesign the Data Protection Board of India to operate independently, without executive interference. Its membership should be judicial and civil society, and its selection process transparent. This will further accountability and public trust in data protection enforcements.
3) **Comprehensive Surveillance Law:** Pass a specific surveillance regulation legislation that outlines the scope, objective, and boundaries of surveillance operations. These laws should be based on the principles of necessity, proportionality, and legality, as indicated by the Supreme Court's ruling in Puttaswamy and global best practices.
4) **Enhance User Rights:** Enhance the Data Principals' rights to cover aspects such as data portability, right to

be forgotten, algorithmic transparency, and the right of explanation in automated decision-making processes. All these rights are important to enable individuals to have more autonomy over their online identities.

5) **Transparency and Reporting:** Make government surveillance activities routine publicly reported, including the volume of data access requests made, granted, and denied. Transparency reports annually will serve to hold authorities accountable, discourage abuses, and enable public discussion on the extent and magnitude of state surveillance.

8. Conclusion

The Digital Personal Data Protection Act, 2023 is a watershed moment for India's transition toward having a formal data[4] governance structure. It brings in core principles like data fiduciaries, consent-based processing, and individual data rights that are fundamental to the age of digital transformation. Nevertheless, the promise of the Act in protecting personal privacy is diluted considerably by blanket exemptions to the state, the absence of strong oversight mechanisms, and the locust-like centralization of regulatory powers in the executive wing.

Under a democracy, the constitutionality of surveillance relies on accountability, proportionality, and transparency. The DPDPA, however, does very little insofar as imposing actual checks on the state's surveillance practices is concerned. Lacking requirements of judicial authorization as well as independent oversight, the law threatens to normalize a surveillance regime that defeats the very purpose it purports to uphold. The erosion of institutional independence—specifically that of the Data Protection Board—is even more troubling in terms of the Act's capacity to serve as a worthy check on abuse.

As India speeds towards a digitally empowered nation through efforts such as Aadhaar, DigiLocker, and IndiaStack, faith in digital infrastructure is essential. That faith can only be maintained through a regime of law that honors the autonomy of the individual and offers transparent recourse against abuse.

Finally, privacy and national security are not a zero-sum situation. It calls for careful legislation that guards people without sacrificing constitutional rights. Enforcing the DPDPA through judicial checks and balances, independent regulatory bodies, and greater transparency is crucial in safeguarding democratic principles in the information age.

References

[1] Ministry of Law and Justice. (2023). The Digital Personal Data Protection Act, 2023. Government of India. https://egazette.nic.in

[2] Srikrishna Committee. (2018). Report of the Committee of Experts on Data Protection. Ministry of Electronics and Information Technology. https://meity.gov.in

[3] Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[4] Internet Freedom Foundation. (2023). Initial analysis of the Digital Personal Data Protection Act, 2023. https://internetfreedom.in

[5] Prasad, R. (2023). India's Data Protection Law: A privacy law or a surveillance enabler? Economic and Political Weekly, 58(33), 10–12.

[6] Bhairav Acharya. (2016). The Four Parts of Privacy in India. Indian Journal of Law and Technology, 12(1), 1–38.

[7] Ramanathan, U. (2023). Digital Personal Data Protection Act: Falling short on constitutional safeguards. The Hindu Centre for Politics and Public Policy. https://thehinducentre.com

[8] Singh, A. (2023). Privacy vs. Security: Evaluating Section 17 of the DPDPA, 2023. National Law School Review, 15(2), 45–59.

[9] Sharma, A. (2024). Surveillance Reform and India's Data Governance Crisis. Journal of Indian Law and Society, 13(1), 88–112.

[10] Centre for Communication Governance. (2023). Policy Brief: DPDPA 2023 and the Future of Privacy in India. National Law University Delhi. https://ccgdelhi.org

[11] Deshmukh, A. (2023). India's Surveillance Infrastructure and the DPDPA: A Missed Opportunity for Oversight. Caravan Magazine. https://caravanmagazine.in

[12] Joshi, M. (2024). Between Rights and Risks: Revisiting India's Data Protection Journey. Observer Research Foundation Occasional Paper No. 421. https://orfonline.org

[13] Freedom House. (2024). Freedom on the Net – India Country Report. https://freedomhouse.org

[14] Trivedi, P. (2023). Aadhaar and Beyond: Data Privacy in India's Public Digital Ecosystem. Indian Public Policy Review, 4(3), 36–52.

[15] Data Governance Network. (2023). Critical Appraisal of India's Digital Personal Data Protection Bill, 2023. https://datagovernance.org

[4] Data Governance Network. (2023). Critical Appraisal of India's Digital Personal Data Protection Bill, 2023. https://datagovernance.org