Privacy Invasion, Surveillance, and State Power in India post DPDP Act, 2023: A Constitutional and Technological analysis. After the 2024-25 Amendments.

By: Ishita Agarwal,

LLB (Hons) 3rd Year

Amity Law School

Amity University, Uttar Pradesh

Abstract

India's data privacy legal framework has significantly transformed following the pivotal decision in Justice K.S. Puttaswamy v. Union of India (2017), which established privacy as a fundamental right under article 21 of the Indian Constitution. This dissertation offers a comprehensive examination of the Digital Personal Data Protection Act (DPDP Act) of 2023, along with its subsequent improvements via The Digital Personal Data Protection (Amendment) Bill of 2024 and the DPDP Rules of 2025. At the heart of this study lies the conflict between the personal control over individual information and the broad surveillance power of the modern state. They study assesses the 2024-25 amendments, which provided detailed definitions for "sensitive personal data", including financial, health, biometric, and genetic information, as well as the "significant harm" principle, aimed at measuring the psychological and social effects of privacy breaches. At the core of the dissertation is analysis of state backed surveillance tech technologies, focusing on the incorporation of artificial intelligence (AI) into the Crime and Criminal Tracking Network and Systems (CCTNS 2.0) for predictive policing, as well as the use of Automated Facial Recognition Systems (AFRS) in public areas. The analysis suggests that "tiered" exemption system under section 17, along with the amendment to section 8(1)(j) of the Right to Information Act (RTI Act), enable a transition from a transparent democracy to a regime characterised by opaque surveillance. By analysing the 2026, constitutional challenge in Venkatesh Nayak v. Union of India, this work investigates the judiciary's pursuit of a "proportionality standard" capable of effectively limiting executive discretionary powers in digital era. The dissertation argues that although the Act establishes a strong foundation for holding the private sector accountable, it creates a notable "legal gap"

concerning state authority, calling for a reassessment of the division of powers and the Data Protection Board of India's responsibility in monitoring state agencies.

Keywords: Privacy, Data Protection, DPDP Act, Fundamental Rights, Surveillance.

Chapter 1: Introduction

1.1 Background of the study

In today's digital era, personal data has become one of the most valuable resources which drives innovation, governance, and economic advancement. With the rapid growth of digital infrastructure, widespread internet access and increase dependency on technology based platforms, The, storing, collection and processing of personal data have become essential for both private as well as public sectors. Initiatives focused on the digital transformation have enhanced and improved the efficiency and accessibility. However, they have also increased concerns about safeguarding and protecting individual privacy.

The rapid increase of tech technologies, such as big data analytics, artificial intelligence and cloud computing has made it possible to process and watch more data than ever before. Private organisations and governments have capability to keep an eye on, monitor, study, analyse, and predict how people will act on large scale. Even though these abilities may serve legitimate purpose and can be used for good reasons, including law enforcement, service delivery, national security, for public good, they also raise serious concerns about over reach, misuse and loss of personal freedom and individual autonomy.[1]

In India, privacy is recognised as a fundamental right under article 21 of the Indian constitution. This was a milestone and a big step forward in constitutional law.[2] Since then the legal landscape has changed to deal and address the challenges that come up from processing digital data. The digital personal data protection act, 2023 represents a big step forward in the law that helps regulating personal data and hold people accountable.[3] However, there are still questions regarding the adequacy of this framework, whether this framework is good enough, especially when it comes to the expanding powers of state surveillance and new and emerging technological risks.

1.2 Concept of Privacy in the Digital Age

In the digital age, privacy has undergone a significant change from what it used to mean: the right to be left alone.[4] It now comprises informational privacy, which basically means how much control people have over their own data. In a society that relies highly on data, personal

---

[1] Neil M Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934.
[2] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
[3] Digital Personal Data Protection Act, 2023.
[4] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 193 (1890).

information is always being collected, gathered, generated and processed often without people being aware of it or giving their full consent.

This digital ecosystem has made it harder to differentiate between private and public spaces.Activities like financial transactions, social media interactions, online communications and even movement patterns are analysed and tracked. This has been a concern and made people worried about spying, surveillance , profiling and manipulating people's behaviour.[5] The growing use of algorithms and automated decision making systems makes the problem even worse ans complicated, since people may have to deal with decisions with no transparency and accountability.

Hence, privacy is no longer just an individual concern but an important element of democratic governance, autonomy and human dignity.[6]

1.3 Emergence of Surveillance and State Power

The growth of digital technologies has made it easier and significantly increased the scope of state surveillance. Government now use a variety of tools, such as interception of communications, biometric identification, systems, artificial intelligence, and monitoring of digital activities. these tools are often used and justified on the grounds of public order, prevention of crime and national security. The information technology act, 2000 in India authorises these power to authorities to intercept, decrypt information, and monitor under certain conditions.[7] In addition to that, the states ability to collect and analyse individual data has also improved because of the integration of large-scale data systems such as identity based databases and infrastructure of public surveillance.[8]

Though surveillance can be useful, and it may serve legitimate purposes, but it's unchecked growth, raises concerns about lack of transparency, not having adequate safeguards, and potential abuse. These concerns are made even worse by the fact that there is absence of any comprehensive law that is specifically regulates surveillance practices.[9] So, the intersection of surveillance and data protection laws, therefore is very important for determining the extent to which individual rights are protected.

---

[5] Daniel J. Solove, Understanding Privacy (Harvard Univ. Press 2008).
[6] Gautam Bhatia, The Transformative Constitution (HarperCollins 2019).
[7] Information Technology Act, No. 21 of 2000, Section 69, India Code (2000).
[8] Ibid.
[9] People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.

1.4 The Digital Personal Data Protection Act, 2023

India's primary legislative framework for controlling and regulating the processing of personal data is the digital personal data protection act, 2023 (DPDP Act). The act talks about the key concepts and ideas like data principals, data, fiduciary, content, based processing, and punishment and penalties for non-compliance. The goal is to establish and find a balance between protecting the privacy of an individual and facilitating and making it easier for the lawful processing of data. however, people have criticised the act, especially the parts and provisions that grant state a lot of exemptions.[10] These exemptions let the government agencies handle and process personal data without following and adhering normal safety rules or standard save cards in some cases and certain circumstances, such as when national security or public order is at stake.[11] These kinds of rules praises concerns about how will the act protects the privacy from the state intrusion and its effectiveness.

Moreover, the lack of independent data protection authority, and the consolidation of regulatory powers within the executive have been recognised as possible vulnerabilities.[12] In the light of rapid technological advancements and increasing Reliance on data driven governance, it becomes important to critically examine whether DPDP act provides appropriate protection to individuals.

1.5 Problem Statement

Although privacy is recognised as a fundamental right and the enactment of DPDP act, 2023 concerns about whether the current legal protections are adequate to prevent privacy, reaches and invasion. The growing scope of state surveillance, combined with technological advancements, like artificial intelligence and data profiling, present serious threats to personal freedom and dignity. The extensive exemption is granted to the state under the DPDP act, along with the absence of strong oversight mechanisms, may lead to an imbalance between State Authority and individual rights. In addition to that, the absence of specific laws governing surveillance practices further undermines the protective framework. This brings up crucial issue regarding whether the existing legal framework adequately protects and save cards. The

[10] Ibid.
[11] Ministry of Electronics & Information Technology, Report of the Committee of Experts on a Data Protection Framework for India (2018).
[12] Parliamentary Standing Committee on Information Technology, Report on Data Security and Privacy (2021).

right to privacy, or if it instead allows for access State surveillance and intrusion in the digital age.

1.6 Research Objectives

- To analyse the constitutional foundation of the right to privacy in India.
- To examine the structure and provisions of DPDP act, 2023.
- To assess the extent of state surveillance and its regulation.
- To examine how emerging technologies affect privacy rights.
- To evaluate if current laws meet constitutional standards.
- To propose and suggest reforms aimed at enhancing privacy protection.

1.7 Research Methodology

This study employees a doctrinal and analytical approach to research. It includes examining and analysing the constitutional provisions, judicial decisions, existing statutes and secondary sources like journal, articles, books, policy, reports, et cetera. And evaluation of India's position has also been conducted through a competitive analysis of international data protection framework. The study also includes technological analysis to assess how new digital tools impact privacy.

1.8 Scope and Limitations

This research is confined to analysing privacy and surveillance under India's legal system, particularly focusing on DPDP act of 2023 and related developments through 2024-2025. Although the text includes references to international frameworks for comparison, the main interest is on Indian law. The research is limited by the ongoing development of technology and data protection regulations, which could result in shifts in the regulatory environment that fall beyond the scope of this research.

Chapter 2: Privacy Jurisprudence in India

2.1 Introduction

In India, the right to privacy has evolved through judicial precedents rather than being explicitly recognised in the constitution. Privacy was not originally recognised as a fundamental right but gradually emerged through a series of significant landmark judgements and court decisions, eventually being acknowledged as an essential part of the right to life and personal ability under article 21 of the Indian constitution.[13] The development of privacy jurisprudence shows the judiciary attempt to balance personal freedom, and individual autonomy with state interests, especially in the context of growing surveillance and technological development.

2.2 Early Judicial Approach to Privacy

The initial constitutional stance regarding privacy in India was unclear, uncertain and fragmented. In Kharak Singh v. state of Uttar Pradesh[14], the Supreme Court assessed the legality of Police surveillance methods, like home visits, and domiciliary visits. The majority held that although some elements of surveillance infringed on personal freedom, the Constitution did not clearly establish a right to privacy. However, Justice Subba Rao, in his descending opinion, strongly advocated for the recognition of privacy as a fundamental aspect of personal liberty. Later, in Gobind v. State of Madhya Pradesh[15], the court took a more progressive approach by acknowledging and recognising that the right to privacy could be derived from article 21. However, the court also stressed that this right was not absolute and could be restricted in the phase of significant state interests. these initial rules set the stage for the evolution of privacy jurisprudence, even though they did not provide a clear constitutional recognition of the right.

2.3 Expansion of Privacy under Article 21

The scope of article 21 has been notably broadened by judicial interpretation, including various aspects of personal freedom, personal, liberty, and dignity. In the case of, Maneka Gandhi v. Union of India[16], the Supreme Court expanded the understanding of "procedure established by law" to encompass, fairness, non arbitrariness, reasonableness. This ruling was crucial in reinforcing The legal framework surrounding fundamental rights and indirectly contributed in

---

[13] Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 S.C.C. 1 (India).
[14] Kharak Singh v. State of UP, AIR 1963 SC 1295 (India).
[15] Gobind v. State of MP,(1975) 2 SCC. 248 (India).
[16] Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India)

acknowledging privacy as a recognised right. Further advancements in cases like R. Rajagopal v. State of Tamil Nadu[17] acknowledged the right to privacy in relation to protection against unauthorised disclosure of personal information. In a similar case, People's Union of Civil Liberties v. Union of India[18], the court addressed, telephone, tapping, and ruled that intercepting communications is a significant breach of privacy, and its invasion, necessitating procedural safeguards. Together, these rulings broaden the scope of privacy and highlighted its role in safeguarding individual autonomy.

2.4 Landmark Judgement: Justice K.S. Puttaswamy v. Union of India (2017)

The most important advancement in privacy law occurred with the ruling in Justice K.S. Puttaswamy (Retd) v. Union of India[19]. A Supreme Court bench consisting of nine judges ruled that the right to privacy is a fundamental right safeguarded under Part III of the Indian Constitution.

The Court acknowledged privacy as an essential aspect of life and personal liberty under Article 21, and also as a component of the freedoms outlined in Article 14 and Article 19. It emphasised that privacy encompasses multiple aspects, including data privacy, bodily privacy, and freedom to make personal decisions.

Significantly, the ruling overturned previous decisions that had rejected the existence of fundamental right to privacy. It also determined that any violation of privacy must satisfy constitutional standards, thus laying the basis for assessing state actions in the digital era.

2.5 The Proportionality Test

A significant contribution of the Puttaswamy judgement is the introduction of the proportionality test, which acts as the standard for evaluating limitations on fundamental rights. The test includes four key components:

- Legitimate Purpose: the action must aim toward a lawful and valid objective.
- Necessity: there needs to be a logical connection between the measure and the objective.
- Proportionality: The extent of interference should be appropriate in relation to the need.
- Procedural Safeguards: appropriate safeguards must exist in place to avoid misuse.

---

[17] R. Rajgopal v. State of Tamil Nadu, (1994) 6 SCC. 632 (India).
[18] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC. 301 (India).
[19] Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India,(2019) 1 SCC. 1 (India).

This framework ensures that any state action that invades privacy undergoes rigorous examination. It is especially important when evaluating surveillance measures and data protection regulations.

2.6 Aadhar Judgement and Informational Privacy

In the case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court assessed the constitutional validity of the Aadhar scheme. While upholding the scheme partially, the Court acknowledged the significance of informational privacy and the dangers linked to large scale data collection.

The Court stressed that data collection should be paired with adequate protections to avoid misuse and guarantee accountability. It also invalidated certain provisions deemed excessive or disproportionate, thus strengthening the application of proportionality test. This ruling emphasised the conflict between welfare measures and privacy rights within a governance system driven by data.

2.7 Privacy and Surveillance: Judicial Perspective

Judicial ruling have repeatedly acknowledged and recognise that surveillance can cause a risk to privacy. In People's Union for Civil Liberties v. Union of India[20], the court established procedural protection for telephone tapping, highlighting the importance of accountability and supervision. More recently, concerns about surveillance were brought up in the context of The Pegasus spyware controversy, where the Supreme Court noted that unauthorised surveillance can have a chilling effect on fundamental rights.[21]

2.8 Critical Analysis of Privacy Jurisprudence

Although acknowledging privacy as a fundamental right is a major accomplishment, various challenges is still exists. The jurisprudence provide robust theoretical safeguard, however, their real world application is often limited. The lack of specific surveillance law, combined with the wide-ranging Authority given to the state, raises concerns regarding possible abuse. In addition to that, the use of the proportionality test is not always uniform, consistent, resulting in uncertainty and ambiguity in judicial rulings. Moreover, rapid technological progress and development has moved faster than legal developments, leading to gaps in regulation. challenges, including artificial intelligence, face, recognition, and data profiling demand,

[20] Ibid.
[21] Manohar Lal Sharma v. Union of India, Writ Petition (Civil) No. 314 of 2021 (Pegasus Case).

specialised legal frameworks and structure that are not yet in place. Therefore, all the privacy law in India has evolved considerably, its ability to deer modern challenges remains.