International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

From Puttaswamy to DPDP: Tracing the Legislative Journey of Data Privacy in India

Dr. Ankit Sourav Sahoo

Assistant Professor (S-II), Lajpat Rai Law College, Sambalpur

Abstract: ***The evolution of data privacy law in India reflects a significant shift in the relationship between technology, governance, and individual rights in the digital age. This article traces the legislative and constitutional journey of data protection in India, beginning from a period when privacy was not explicitly recognised as a fundamental right to the enactment of a comprehensive legal framework under the DPDP Act, 2023. The study highlights how rapid digitalisation, increasing reliance on data-driven technologies, and the growing economic value of personal data have intensified concerns regarding surveillance, data misuse, and individual autonomy. A major turning point in this journey was the landmark judgment in Puttaswamy Case (2017), where the Supreme Court recognised privacy as a fundamental right under Article 21 of the Constitution. This decision laid the constitutional foundation for data protection and established key principles such as legality, necessity, and proportionality. The article further examines subsequent legislative efforts, including the recommendations of the Srikrishna Committee and the evolution of draft data protection bills, culminating in the enactment of the Digital Personal Data Protection Act, 2023. While the Act introduces a consent-based framework, defines roles such as data principal and data fiduciary, and establishes the Data Protection Board of India, it also raises concerns regarding government exemptions, limitations on transparency, and practical challenges in implementation. The study concludes that although India has made substantial progress in establishing a data protection regime, continuous reforms and judicial oversight are essential to balance innovation with the protection of fundamental rights in the digital era.***

Keywords: Data Protection, Privacy, Information Technology, Digital Security, Data Protection Board

1. Introduction

For decades, legislators, economists, and technology entrepreneurs have reiterated a compelling metaphor: “data is the new oil.” The comparison illustrates the substantial economic value derived from the collection, processing, and analysis of digital information in the contemporary economy. Technology firms depend on extensive amounts of customer data to enhance services, train algorithms, and produce targeted advertising income. Governments are increasingly reliant on digital databases to provide welfare payments, oversee public services, and enhance national security infrastructure. In this regard, data has become an essential resource in the operation of the digital era. However, the metaphor is inherently deficient. In contrast to oil or other natural resources, data transcends being a mere traded commodity; it is intricately linked to the identity, autonomy, and dignity of humans.

Each digital transaction generates remnants of personal information. An individual's search history, biometric information, financial transactions, geolocation data, medical records, and social media interactions collectively constitute a comprehensive digital profile. When gathered and examined, such information might disclose private facets of an individual's life, encompassing personal habits, political beliefs, health status, and social connections. Thus, data governance has transcended mere economic policy or technological advancement; it has emerged as a critical concern about civil liberties and constitutional rights.

The past decade of India's experience eloquently exemplifies this transition. The nation has experienced an unparalleled growth of its digital environment. India has become one of the largest digital societies globally, boasting over a billion mobile connections, a swiftly expanding internet user base, and extensive government efforts including digital identity systems and online public services. As millions of individuals engage with digital platforms daily be it for banking, education, healthcare, or social networking the quantity of personal data created has increased dramatically. This development has generated significant prospects for economic expansion and technological progress, however it has also posed substantial threats about surveillance, data breaches, and the misuse of personal information.

Until recently, India did not possess a comprehensive legislative framework for the protection of personal data. Early constitutional jurisprudence regarded privacy with ambiguity, and statutory protections were confined to specific provisions within technology legislation. Consequently, enquiries regarding the collection, storage, and utilisation of personal data mostly remained unanswered. The situation underwent significant transformation in 2017 when the Supreme Court of India acknowledged the right to privacy as a fundamental right enshrined in the Constitution. The historic ruling not only changed the constitutional interpretation of privacy but also initiated a comprehensive legislative endeavour to control the swiftly advancing data economy.

This article delineates the legislative and constitutional progression that ensued. This analysis commences with the pre-2017 legislative environment and scrutinises the evolution of Indian privacy law through significant judicial rulings, expert committee recommendations, and parliamentary discussions. The discourse thereafter examines the implementation of the Digital Personal Data Protection Act, 2023, India's inaugural comprehensive legislation focused exclusively on data protection. The law marks a notable advancement in India's digital governance framework, yet it has sparked extensive discourse among academics, policymakers, and civil society organisations concerning its scope, efficacy, and ramifications for

democratic accountability.

Comprehending this transformation is crucial not only for legal practitioners and policymakers but also for everyday citizens engaged in the digital economy. In a time when personal information is pivotal to economic and political influence, the inquiry shifts from whether data regulation is necessary to how such regulation may harmonise innovation, governance, and the safeguarding of individual rights.

Significance of Right to Privacy in Indian Context

The concept of the Right to Privacy might sound like a complex legal term, but it is actually one of the most important parts of being a free human being. In India, the Supreme Court has made it clear that privacy is a fundamental right. At its heart, privacy is about Human Dignity. This means that every person deserves a private space where they aren't being watched or judged by the government or the public. Without this space, we can't feel truly respected or "at home" in our own lives. It is the foundation that allows us to live with self-respect, knowing that our private thoughts and moments belong only to us.

Privacy is also the key to Individual Autonomy, which is a fancy way of saying "the power to make your own choices." Think about the biggest decisions in life, like who you want to marry, what career you want to follow, or how you want to live your daily life. If the state or society is always looking over your shoulder, you might feel pressured to make choices just to please others. Privacy acts like a shield, giving you the freedom to decide what is best for you without anyone else interfering in your personal business.[1]

Another big reason privacy matters is that it protects our Freedom of Expression. Have you ever noticed how people act differently when they know a camera is watching them? This is called a "chilling effect." If we feel like the government is constantly monitoring our messages or internet searches, we might become too afraid to speak our minds or learn about new, different ideas. Privacy ensures that our "inner world" stays safe, so we can grow, ask questions, and express ourselves honestly without fear of being punished for simply thinking differently.[2]

Finally, in today's world, privacy is our best defense for Digital Security. Since we spend so much time on phones and computers, almost everything about us from our bank details to our private photos is stored as data. If this information isn't kept private, it can be stolen by hackers or misused by big companies through "data harvesting." Protecting our digital privacy isn't just about keeping secrets; it's about keeping our money safe, protecting our identity from being stolen, and making sure our mental well-being isn't hurt by online harassment.

The Pre-Puttaswamy Era: When Privacy was a "Privilege"

Prior to 2017, if one enquired of a lawyer, "Do I possess a fundamental right to privacy in India?" the response would have been, "It is complex." During the initial years of the Indian Republic, the Supreme Court exhibited a conservative stance regarding privacy. Two significant cases established the precedent:

1) M.P. Sharma v. Satish Chandra (1954)[3]: The court determined that the Constitution does not explicitly safeguard a "right to privacy." This case pertained to police search and seizure operations.
2) Kharak Singh v. State of Uttar Pradesh (1962)[4]: In this case, the police maintained a "history sheet" on an individual, surveilling his residence at night and disturbing his sleep. The Court determined that although "domiciliary visits" (police intrusions) were improper, a universal "right to privacy" does not exist under the Constitution.

Upon the advent of the internet in India, the government recognised the necessity for regulatory measures. The Information Technology (IT) Act was enacted in 2000.

- Section 43A: This provision was subsequently incorporated to stipulate that if a corporation manages "sensitive personal data" and neglects to safeguard it, they are liable to provide compensation.
- The Issue: This was exceedingly narrow. It exclusively pertained to "corporate entities," excluding the government. It concentrated solely on "compensation" rather than "prevention." If a corporation compromised your data, you were required to demonstrate that you incurred a "loss" to receive any compensation. In the digital era, how can you assign a monetary value to a leaked private photograph or a compromised location history?

The Puttaswamy Watershed: The Catalyst of Privacy

In 2017, a transformation occurred. A 91-year-old retired judge, Justice K.S. Puttaswamy, contested the government's Aadhaar initiative.[5] He contended that mandating Aadhaar for all purposes infringed upon his privacy.

The government's attorneys contended in court that the Constitution does not enshrine privacy as a fundamental right. This compelled the Supreme Court to establish a substantial nine-judge panel to resolve the matter definitively. The Court rendered a majority decision: Privacy constitutes a Fundamental Right. It is safeguarded by Article 21 (The Right to Life and Liberty). The judges notably remarked that "privacy is the paramount manifestation of individual sanctity."

The Court recognised that no right is unconditional. The government may limit your privacy, but only if it overcomes three obstacles: An existing legislation must be established. A mere executive order is insufficient. The government must

[1] Richards, Neil, 'Identity', *Why Privacy Matters* (New York, 2022; online edn, Oxford Academic, 18 Nov. 2021), https://doi.org/10.1093/oso/9780190939045.003.0005, accessed 16 Mar. 2026.
[2] Otoya, S. J. (2019, December 1). *Chilling Effects of Surveillance, Freedex*. Freedex. https://freedex.org/2019/12/01/chilling-effects-of-surveillance/
[3] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India)
[4] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India)
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India)

possess a valid justification, such as national security or the allocation of food rations. The infringement on privacy must be the "least restrictive" means to attain the objective. One cannot employ a sledgehammer to break a nut. Following the Puttaswamy judgement, the Supreme Court instructed the government: "Proceed to enact a comprehensive law." This initiated a five-year cycle of "draft and delete."

The Srikrishna Committee, established in 2018[6]
The government designated Justice B.N. Srikrishna to lead a committee. They generated a draft that was notably "pro-consumer." It established notions such as Data Sovereignty (retaining Indian data within India).

The 2019 Legislation and the Joint Parliamentary Committee
The government modified the Srikrishna draft. The Personal Data Protection Bill, 2019[7] was presented in Parliament but promptly encountered criticism. What is the reason? It conferred substantial authority to the government to relieve itself from legal obligations. A Joint Parliamentary Committee (JPC) conducted a two-year study and proposed 81 modifications. In August 2022, the government withdrew the law outright due to its complexity, pledging to present a "fresh, modern" version.

Critical Examination of the DPDP Act, 2023:
The Digital Personal Data Protection (DPDP) Act was enacted in August 2023.[8] It is far more concise and straightforward than earlier iterations; yet, simplicity does not always equate to superiority.

Essential Definitions:
To comprehend the Act, it is essential to be familiar with the "Participants":
- Data Principal: That refers to you. The person from whom data is being gathered.
- Data Fiduciary: The organization or entity (such as Instagram, a financial institution, or an educational institution) that determines the purposes and methods of data processing.
- Data Processor: An external entity that manages data on behalf of the Fiduciary, such as a cloud storage provider.

The Consent-Centric Paradigm: The Act stipulates that organisations may only collect personal data with "free, specific, informed, unconditional, and unambiguous" consent. A "Notice" must be provided in clear language, including regional Indian languages, detailing the data being collected.

The Reality Check: Have you ever thoroughly examined the "Terms and Conditions"? The majority of individuals only select "I Agree." Critics contend that the "Consent" paradigm is illusory, as consumers possess no genuine option refusal to accept precludes app usage.

The Data Protection Board (DPB): The Act establishes a new entity known as the Data Protection Board of India. Consider them as the "Arbiters." If a firm breaches your data or infringes upon your rights, you may file a complaint with the Data Protection Board (DPB). They has the authority to impose substantial penalties on companies up to ₹250 Crore (about $30 million) each occurrence.

Discrepancies and Issues:

Although the Act is commendable in theory, legal scholars have identified several concerns.

1) Extensive Government Exemptions (Section 7)
Section 7 permits the government to handle your data without your consent for "legitimate purposes." This encompasses activities such as preserving public order or administering subsidies. Critics apprehend that this constitutes a "backdoor" for governmental spying. Does the "Three-fold Test" of the Puttaswamy judgement still applicable if the government is not bound by the same regulations as private enterprises?

2) Erosion of the RTI Act
The Right to Information (RTI) Act of 2005 serves as a mechanism for citizens to ensure governmental accountability. The DPDP Act amends the RTI Act to stipulate that "personal information" is rarely permissible for disclosure. Although this appears to safeguard privacy, it may be exploited by corrupt officials to conceal their assets or obscure the recipients of government contracts under the pretext of personal information.

3) The Responsibilities of the Data Principal
Interestingly, the Act delineates specific "Duties" for you. Submitting false information or lodging a "frivolous" complaint may result in a fine of up to ₹10,000. Some contend that this may deter individuals from reporting data breaches due to the concern of incurring fines themselves.

2. Conclusion

The progression from acknowledging privacy as a constitutional right to the implementation of a comprehensive data protection law represents a pivotal advancement in India's contemporary legal framework. In the last ten years, the nation has transitioned from a disjointed and ambiguous regulatory framework to a more organised methodology for the governance of personal data. This transition signifies a wider worldwide trend wherein nations are progressively acknowledging that digital technology, whilst facilitating economic advancement and administrative efficacy, have accompanying safeguards to defend individual rights and democratic principles. The constitutional acknowledgement of privacy in 2017 dramatically transformed the course of data governance in India. The Supreme Court set a normative foundation for future regulation by asserting that privacy is an integral component of the right to life and personal liberty. The ruling underscored that individual autonomy, informational self-determination, and human dignity must be paramount in any regulatory system concerning personal data. It established the notion that privacy limits must meet criteria of legality, necessity, and proportionality, thus offering a

[6] Ministry of Electronics & Information Technology, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

[7] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Lok Sabha (India)

[8] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Aug. 11, 2023)

constitutional standard for assessing future official acts.

Subsequent years witnessed numerous legislative initiatives aimed at codifying these constitutional ideas into statute law. Expert committees, parliamentary discussions, and public consultations collectively influenced the discourse on India's regulation of data in the digital era. Despite earlier suggestions encountering criticism and being subsequently retracted, they significantly contributed to the refinement of policy strategies and underscored critical issues such as data localisation, regulatory monitoring, and governmental access to personal information.

The Digital Personal Data Protection Act, 2023 signifies the conclusion of this extended legislative endeavour. The Act explicitly acknowledges individuals as "data principals" and mandates responsibilities for companies that handle personal information, so creating India's inaugural complete framework for personal data protection. The stipulations about consent, transparency, and financial sanctions for non-compliance indicate a transition towards enhanced accountability in the digital ecosystem. The establishment of the Data Protection Board introduces an institutional structure aimed at resolving disputes and ensuring legal compliance. Nonetheless, the Act has sparked significant discourse concerning its enduring efficacy. Critics have expressed apprehensions regarding the extensive nature of government exclusions, the possible repercussions for transparency within the Right to Information framework, and the pragmatic difficulties linked to implementing consent-based data governance in a multifaceted digital marketplace. The aforementioned concerns indicate that the DPDP Act ought to be seen not as the culmination of India's data protection evolution, but as a significant inception in the advancement of a more sophisticated legal framework. As digital technologies like artificial intelligence, predictive analytics, and biometric identification proliferate, the quantity and sensitivity of personal data processed will rise substantially. This reality will eventually challenge the robustness of current legal frameworks and necessitate ongoing adaptation via judicial interpretation, regulatory monitoring, and legislative reform. The concepts established in the privacy judgement and the institutional frameworks implemented by the DPDP Act will be essential in determining the future of digital rights in India. The ultimate success of India’s data protection framework will hinge on its capacity to achieve a nuanced equilibrium: fostering innovation and digital advancement while safeguarding the constitutional guarantees of individual freedom, dignity, and autonomy in the information era.