IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

Review on Present Data Protection Act in India: Issues and Challenges

Bhavika Sisodia
Student of LLM 2nd Year, Sem IV
School of Law, Sandip University, Nashik

Abstract: *The rapid expansion of digital technologies has significantly increased the volume of personal data being collected, processed, and stored by both governmental and private entities. In India, growing concerns regarding privacy, data misuse, and unauthorized surveillance led to the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act). This research paper critically evaluates the present data protection framework in India by examining the provisions and effectiveness of the DPDP Act. Furthermore, it explores the challenges in implementation, including low public awareness, technological complexities, and compliance burdens on organizations. The study concludes by suggesting reforms aimed at strengthening India's data protection regime in alignment with global standards like the GDPR, thereby ensuring a balance between innovation and individual privacy.*

Keywords: Data Protection, Privacy, DPDP Act 2023, Data Fiduciary, Data Principal, Cyber Law, India, GDPR

I. INTRODUCTION

In the contemporary digital era, personal data has emerged as a crucial economic and social resource, often described as the "new oil" due to its immense value. The increasing dependence on digital platforms for communication, commerce, governance, and social interaction has led to significant concerns regarding the protection of personal information. The recognition of the right to privacy as a fundamental right by the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India (2017) marked a transformative moment in Indian constitutional jurisprudence. This landmark judgment emphasized the necessity of protecting individual autonomy and informational privacy in a digital society. In response to these developments, the Indian legislature enacted the Digital Personal Data Protection Act, 2023, which represents the country's first comprehensive attempt to regulate the processing of personal data. The Act establishes a legal framework based on consent, accountability, and transparency, defining the roles of data fiduciaries and data principals while providing individuals with rights such as access, correction, and erasure of data. However, despite its significance, the Act has been subject to criticism for various shortcomings. This paper seeks to critically analyze the Act, focusing on its issues and challenges while assessing its effectiveness in safeguarding privacy rights. The evolution of data protection law in India has been gradual and shaped by both domestic and global developments.

Initially, the Information Technology Act, 2000 provided limited safeguards against data misuse, primarily through Section 43A, which imposed liability on companies for negligence in handling sensitive personal data. The subsequent introduction of the Sensitive Personal Data or Information Rules, 2011 further elaborated on these protections, though their scope remained narrow and enforcement weak. A major turning point occurred with the establishment of the Justice B.N. Srikrishna Committee in 2017, which was tasked with examining issues relating to data protection and recommending a comprehensive legal framework. The Committee's report in 2018 laid the foundation for the Personal Data Protection Bill, 2019, which sought to introduce robust safeguards and regulatory mechanisms. However, due to extensive criticism and concerns over its provisions, the Bill was eventually withdrawn. The enactment of the Digital Personal Data Protection Act, 2023 marked a new phase in India's data protection journey. While the Act simplifies certain aspects and focuses specifically on digital personal data, it also departs from earlier drafts by omitting key features such as the classification of sensitive data, thereby raising concerns about the adequacy of protection. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

literature on the Digital Personal Data Protection Act, 2023 highlights both its strengths and limitations. Scholars view the Act as an important step toward protecting privacy in India's digital economy through a structured data protection framework and recognition of individual rights. However, concerns remain regarding broad government exemptions, lack of safeguards for sensitive personal data, and challenges in implementation such as limited institutional capacity and low public awareness. Overall, researchers believe the Act is progressive but requires further improvements for effective data protection.

ISSUES IN THE PRESENT DATA PROTECTION ACT

One of the most significant issues associated with the Digital Personal Data Protection Act, 2023 is the broad scope of exemptions granted to the government. The Act allows the central government to exempt its agencies from compliance on grounds such as national security, public order, and sovereignty, which raises serious concerns regarding potential misuse and lack of oversight. Another critical issue is the absence of a distinct category for sensitive personal data, such as health, financial, or biometric information. This omission weakens the level of protection afforded to individuals and exposes them to greater risks. Furthermore, the Act has been criticized for its lack of transparency and accountability mechanisms, as it does not provide sufficient checks on the actions of data fiduciaries or the government. The amendment to the Right to Information Act through the DPDP framework also poses challenges, as it may restrict access to information by classifying it as personal data, thereby affecting transparency in governance. Additionally, the concept of consent under the Act may lead to "consent fatigue," where individuals routinely accept terms without fully understanding them, undermining the principle of informed consent.

CHALLENGES IN IMPLEMENTATION

The implementation of the Digital Personal Data Protection Act, 2023 presents several practical challenges that may hinder its effectiveness. One of the primary challenges is the establishment and functioning of the Data Protection Board of India, which is responsible for enforcement and adjudication. The Board may face limitations in terms of resources, expertise, and independence, affecting its ability to regulate effectively. Another significant challenge is the lack of awareness among citizens regarding their data protection rights, which limits the practical utility of the law. Compliance with the Act may also impose a considerable burden on businesses, particularly small and medium enterprises, which may lack the necessary infrastructure and expertise to adhere to complex requirements. Cross-border data transfer presents another challenge, as the Act allows transfers to notified countries without clearly defining adequacy standards or safeguards. Additionally, the rapid advancement of technologies such as artificial intelligence, big data analytics, and surveillance systems creates new risks that the Act does not fully address, thereby necessitating continuous updates and reforms.

II. CONCLUSION

The Digital Personal Data Protection Act, 2023 represents a significant milestone in India's efforts to establish a comprehensive data protection framework in the digital age. It reflects the growing recognition of privacy as a fundamental right and introduces important mechanisms for regulating the processing of personal data. However, the Act is not without its limitations, as it suffers from issues such as broad government exemptions, lack of safeguards for sensitive data, and challenges in implementation. The effectiveness of the Act will ultimately depend on its enforcement, institutional capacity, and the willingness of policymakers to address its shortcomings. In conclusion, while the DPDP Act lays a strong foundation for data protection in India, it requires continuous refinement and reform to ensure that it adequately balances the interests of individuals, businesses, and the state in an increasingly digital society.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

SUGGESTIONS

In order to address the issues and challenges associated with the Digital Personal Data Protection Act, 2023, several reforms can be proposed. Firstly, it is essential to strengthen the institutional framework by ensuring the independence, capacity, and accountability of the Data Protection Board. Secondly, the scope of government exemptions should be clearly defined and subjected to judicial oversight to prevent misuse. Thirdly, the Act should reintroduce the classification of sensitive personal data and provide enhanced safeguards for such information. Furthermore, greater transparency can be achieved by implementing robust mechanisms for audits, reporting, and public accountability. There is also a need to promote public awareness and digital literacy through targeted campaigns, enabling individuals to understand and exercise their rights effectively. Finally, aligning the Indian data protection framework with international standards such as the GDPR would facilitate global data flows and enhance the credibility of the system.

BIBLIOGRAPHY

[1]. The Digital Personal Data Protection Act, 2023 (India).
[2]. The Information Technology Act, 2000 (India).
[3]. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[4]. Justice B.N. Srikrishna Committee Report on Data Protection, 2018.
[5]. Personal Data Protection Bill, 2019 (India).
[6]. General Data Protection Regulation (EU), 2018.
[7]. Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Government of India, 2018).
[8]. Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014).
[9]. Paul Voigt & Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer, 2017).
[10]. Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013).
[11]. Lee A. Bygrave, Data Privacy Law: An International Perspective (Oxford University Press, 2014).