



ICHSECMICE -2025

11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

Data Privacy and Digital Rights in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023,

Mr.Sukrut Deo, Ph.D Scholar; MIT ADT University, Pune
Dr Govind Singh Rajpal, Research Guide, MIT ADT University, Pune

Introduction

The rapid advancement of digital technologies has transformed the manner in which individuals communicate, conduct business, access public services, and interact with digital platforms. The increasing use of smartphones, social media networks, e-commerce platforms, cloud computing, and artificial intelligence has resulted in the generation and processing of vast amounts of personal data. In the digital age, personal information has become a valuable asset, making data protection and privacy critical concerns for individuals, businesses, and governments alike (1,2).

The growing dependence on digital technologies has created significant opportunities for economic development and innovation. However, it has also increased the risks associated with unauthorized collection, misuse, disclosure, and exploitation of personal information. Incidents involving data breaches, identity theft, cyber fraud, surveillance, and unauthorized profiling have highlighted the vulnerability of personal data in the digital environment. These challenges have intensified the demand for robust legal mechanisms to safeguard privacy and protect individual rights (3,4).

In India, the recognition of privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) marked a significant milestone in the development of privacy jurisprudence. The judgment emphasized the importance of informational privacy and underscored the need for a comprehensive data protection framework capable of addressing emerging technological challenges (5).

Responding to these concerns, the Government of India enacted the Digital Personal Data Protection Act, 2023 with the objective of regulating the processing of personal data while balancing individual privacy rights and legitimate business interests. The legislation establishes rights for individuals, obligations for entities processing personal data, and mechanisms for enforcement and accountability. The Act seeks to create a transparent and secure framework for data governance in India's rapidly expanding digital economy (6,7).

Despite its significance, the Digital Personal Data Protection Act, 2023 has generated considerable debate regarding its scope, effectiveness, exemptions, enforcement mechanisms, and implications for digital rights. Therefore, a critical examination of the legislation is necessary to assess its ability to protect privacy, promote accountability, and address contemporary challenges arising from the digital ecosystem.

The present study analyses the concept of data privacy and digital rights, examines the key provisions of the Digital Personal Data Protection Act, 2023, evaluates its strengths and limitations, and explores its implications for individuals, businesses, and governance in India.

Concept of Data Privacy and Digital Rights

Data privacy refers to the right of individuals to control the collection, use, storage, processing, and disclosure of their personal information. In the digital age, personal data has become a valuable resource that is extensively collected by governments, businesses, social media platforms, financial institutions, and online service providers. Data privacy seeks to ensure that such information is handled lawfully, fairly, and transparently while protecting individuals from unauthorized access, misuse, or exploitation of their personal information (8,9).

The importance of data privacy has increased significantly with the rapid growth of digital technologies and internet-based services. Consumers routinely share sensitive information such as names, addresses, financial details, health records, biometric data, and online behavioural

International Advance Journal of Engineering, Science and Management (IAJESM)

Multidisciplinary, Multilingual, Indexed, Double-Blind, Open Access, Peer-Reviewed, Refereed-

International Journal, Impact factor (SJIF) = 8.152



ICHSECMICE -2025 11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

patterns while interacting with digital platforms. In the absence of adequate safeguards, such information may be vulnerable to cyberattacks, identity theft, unauthorized profiling, surveillance, and data breaches. Consequently, data privacy has emerged as a fundamental component of individual autonomy, dignity, and personal security in the digital environment (10,11).

Digital rights refer to the rights and freedoms that individuals possess while using digital technologies and online platforms. These rights are derived from traditional human rights principles and extend to the digital sphere. They include the right to privacy, the right to access information, the right to freedom of expression, the right to data protection, the right to online security, and the right to seek remedies against digital harms. The protection of digital rights is essential for ensuring that technological advancements do not undermine individual freedoms and democratic values (12).

In contemporary society, data privacy and digital rights are closely interconnected. Effective protection of personal data strengthens consumer trust, promotes responsible innovation, and enhances accountability among organizations that process personal information. As digital technologies continue to evolve, safeguarding privacy and digital rights remains essential for maintaining a secure, transparent, and rights-based digital ecosystem (13,14).

Evolution of Data Protection Laws in India

The evolution of data protection laws in India reflects the country's transition towards a digital economy and the increasing recognition of privacy as a fundamental right. Prior to the enactment of a dedicated data protection legislation, issues relating to personal data and privacy were primarily governed through constitutional principles, contractual obligations, and limited statutory provisions. The absence of a comprehensive legal framework often resulted in uncertainty regarding the rights of individuals and the responsibilities of organizations handling personal information (15,16).

The Information Technology Act, 2000 was the first significant legislation addressing electronic transactions and cyber-related activities in India. Although the Act primarily focused on e-commerce and cybercrimes, it also introduced provisions relating to data protection through Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These provisions imposed obligations on organizations to implement reasonable security measures for protecting sensitive personal information (17,18).

A major development in India's privacy jurisprudence occurred in 2017 when the Supreme Court, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized that informational privacy is an essential aspect of individual liberty and highlighted the need for a comprehensive data protection framework. This landmark decision significantly influenced subsequent legislative developments relating to privacy and personal data protection (19).

Following the Puttaswamy judgment, various committees and expert groups examined the need for dedicated data protection legislation. The Justice B.N. Srikrishna Committee submitted its report in 2018 and recommended a comprehensive framework for the protection of personal data. These recommendations eventually contributed to the enactment of the Digital Personal Data Protection Act, 2023, which represents India's first comprehensive legislation specifically dedicated to regulating the processing of personal data and protecting privacy rights in the digital age (20,21).

The enactment of the Digital Personal Data Protection Act, 2023 marks a significant step towards strengthening privacy protection and promoting responsible data governance in India.

International Advance Journal of Engineering, Science and Management (IAJESM)

Multidisciplinary, Multilingual, Indexed, Double-Blind, Open Access, Peer-Reviewed, Refereed-

International Journal, Impact factor (SJIF) = 8.152





ICHSECMICE -2025 11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

The legislation seeks to balance individual rights with innovation, economic development, and legitimate governmental interests, thereby establishing a structured framework for data protection in an increasingly digital society (22).

Key Provisions of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 establishes a comprehensive framework governing the processing of personal data in India. The Act applies to digital personal data collected within India and, in certain circumstances, to data processing activities conducted outside India where goods or services are offered to individuals within the country. The legislation seeks to ensure lawful processing of personal data while safeguarding the privacy rights of individuals (23).

One of the central features of the Act is the requirement of consent-based data processing. Personal data may be processed only for lawful purposes and after obtaining free, specific, informed, unconditional, and unambiguous consent from the individual concerned. The Act also recognizes certain legitimate uses where consent may not be necessary under specified circumstances (24).

The legislation grants various rights to Data Principals, including the right to access information regarding data processing, the right to correction and erasure of personal data, the right to grievance redressal, and the right to nominate another person to exercise such rights when required. These provisions strengthen individual control over personal information and promote transparency in data handling practices (25).

The Act imposes several obligations upon Data Fiduciaries responsible for processing personal data. Such entities must implement appropriate security safeguards, ensure accuracy of information, notify data breaches, and adopt measures to prevent unauthorized access or misuse of personal information. Significant Data Fiduciaries may also be subject to additional compliance requirements due to the nature and scale of their data processing activities (26).

The legislation establishes the Data Protection Board of India to oversee compliance, investigate violations, and impose penalties for non-compliance. The availability of substantial monetary penalties seeks to encourage accountability and responsible data governance among organizations processing personal data (27).

Rights and Duties of Data Principals

The Digital Personal Data Protection Act, 2023 recognizes individuals as Data Principals and grants them specific rights relating to their personal information. These rights seek to ensure transparency, accountability, and individual autonomy in the digital environment (28).

A Data Principal has the right to obtain information regarding the processing of personal data, including the categories of information collected, the purpose of processing, and the entities with whom such information may be shared. The Act also provides the right to correction, completion, updating, and erasure of personal data where appropriate (29).

Individuals are entitled to access grievance redressal mechanisms and may approach the Data Protection Board if their concerns are not adequately addressed. Furthermore, the Act provides the right to nominate another individual to exercise data-related rights in specified circumstances (30).

Alongside these rights, Data Principals are expected to comply with certain duties, including providing authentic information, refraining from impersonation, and avoiding false or frivolous complaints. These duties contribute to the effective functioning of the data protection framework (31).

Obligations of Data Fiduciaries

Data Fiduciaries are organizations, businesses, government bodies, or other entities that determine the purpose and means of processing personal data. The Act places significant

International Advance Journal of Engineering, Science and Management (IAJESM)

Multidisciplinary, Multilingual, Indexed, Double-Blind, Open Access, Peer-Reviewed, Refereed-

International Journal, Impact factor (SJIF) = 8.152





ICHSECMICE -2025 11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

responsibilities upon such entities to ensure lawful and secure processing of personal information (32).

Data Fiduciaries must process personal data only for lawful purposes and in accordance with valid consent or other legally recognized grounds. They are required to maintain reasonable security safeguards, implement measures to prevent data breaches, and ensure timely reporting of incidents involving unauthorized access or disclosure of personal information (33).

The legislation further requires Data Fiduciaries to erase personal data when the purpose of processing has been fulfilled unless retention is mandated by law. They must also establish effective grievance redressal mechanisms and facilitate the exercise of rights by Data Principals (34).

These obligations promote responsible data governance and encourage organizations to adopt privacy-focused business practices in the digital economy (35).

Challenges and Criticisms of the Act

Despite its significance, the Digital Personal Data Protection Act, 2023 has attracted criticism from legal scholars, privacy advocates, and civil society organizations. One major concern relates to the broad exemptions available to government agencies under certain circumstances. Critics argue that such exemptions may affect the balance between privacy rights and state interests (36).

Another concern involves the absence of an independent data protection authority. While the Act establishes the Data Protection Board of India, questions have been raised regarding its autonomy and effectiveness in ensuring impartial oversight and enforcement (37).

The legislation has also been criticized for limited provisions relating to data portability, automated decision-making, and algorithmic transparency. As emerging technologies increasingly influence decision-making processes, these areas may require further regulatory attention (38).

Cross-border data transfers, enforcement challenges, and varying levels of digital literacy among citizens also present practical difficulties in the implementation of the legislation. Addressing these concerns will be essential for achieving the objectives of effective privacy protection and responsible data governance (39).

Critical Analysis

The Digital Personal Data Protection Act, 2023 represents a significant advancement in India's privacy framework and reflects the growing importance of data protection in the digital age. The legislation provides a structured mechanism for regulating personal data processing and recognizes privacy as an essential aspect of individual autonomy and dignity (40).

The Act successfully introduces rights-based protections and establishes obligations for organizations handling personal data. However, its effectiveness will largely depend upon implementation, enforcement, institutional independence, and public awareness. Certain provisions relating to exemptions, oversight mechanisms, and technological regulation may require further refinement to ensure a stronger balance between innovation, governance, and privacy rights (41).

Therefore, while the Act constitutes a major step forward, continuous evaluation and adaptation will be necessary to address emerging challenges in an evolving digital ecosystem.

Findings

1. Data privacy has emerged as a critical concern in the digital economy.
2. The Digital Personal Data Protection Act, 2023 provides India's first comprehensive data protection framework.
3. The Act strengthens individual rights relating to personal information.



ICHSECMICE -2025 11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

4. Organizations are subject to enhanced obligations concerning data processing and security.
5. Privacy protection contributes to consumer confidence and digital trust.
6. Enforcement and implementation challenges remain significant.
7. Certain provisions continue to generate debate regarding privacy and governmental powers.

Suggestions

1. Strengthen institutional independence of enforcement authorities.
2. Enhance public awareness regarding privacy rights and data protection.
3. Develop comprehensive guidelines relating to artificial intelligence and automated decision-making.
4. Promote transparency in algorithmic processing and profiling activities.
5. Encourage privacy-by-design practices among organizations.
6. Strengthen cyber security standards and incident response mechanisms.
7. Periodically review and update legislation to address emerging technological developments.

Conclusion

The Digital Personal Data Protection Act, 2023 marks a significant milestone in India's journey towards establishing a robust data protection regime. By recognizing the importance of privacy and creating a framework governing the processing of personal data, the legislation seeks to protect individuals while supporting innovation and economic growth.

As digital technologies continue to evolve, effective protection of personal data will remain essential for safeguarding individual rights, maintaining public trust, and ensuring responsible digital governance. Although certain challenges and criticisms persist, the Act provides a strong foundation for the development of a privacy-conscious digital ecosystem in India. Continuous reforms, effective enforcement, and greater public awareness will be crucial for realizing the full potential of the legislation and strengthening digital rights in the years ahead.

References

1. OECD. (2024). *Consumer Policy and the Digital Transformation*. Paris: OECD Publishing.
2. United Nations Conference on Trade and Development (UNCTAD). (2024). *Digital Economy Report 2024*. Geneva: United Nations Publications.
3. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. Geneva: World Economic Forum.
4. European Union Agency for Cybersecurity (ENISA). (2024). *Data Protection and Privacy Challenges in the Digital Era*. Brussels.
5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
6. Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)*. New Delhi: Ministry of Law and Justice.
7. Ministry of Electronics and Information Technology (MeitY). (2023). *Explanatory Note on the Digital Personal Data Protection Act, 2023*. New Delhi: Government of India.
8. Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220.
9. Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Cambridge, MA: Harvard University Press.
10. OECD. (2024). *Consumer Policy and the Digital Transformation*. Paris: OECD Publishing.



ICHSECMICE -2025 11-12th October 2025

Sardar Patel Institute of Higher Education, Kurukshetra

11. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Geneva: World Economic Forum.
12. United Nations Human Rights Council. (2023). The Right to Privacy in the Digital Age. Geneva: United Nations.
13. Government of India. (2023). The Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Law and Justice.
14. European Union. (2018). General Data Protection Regulation (GDPR). Brussels: European Union.
15. Basu, D. D. (2021). Introduction to the Constitution of India (25th ed.). New Delhi: LexisNexis.
16. Solove, D. J. (2021). Understanding Privacy (2nd ed.). Cambridge, MA: Harvard University Press.
17. Government of India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000). New Delhi: Ministry of Law and Justice.
18. Government of India. (2011). Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. New Delhi: Ministry of Electronics and Information Technology.
19. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
20. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. New Delhi: Government of India.
21. Government of India. (2023). The Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Law and Justice.
22. Ministry of Electronics and Information Technology (MeitY). (2023). Explanatory Note on the Digital Personal Data Protection Act, 2023. New Delhi: Government of India.
23. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
24. Ministry of Electronics and Information Technology. (2023). *Explanatory Note on the Digital Personal Data Protection Act, 2023*.
25. Bhandari, M. (2024). Data Privacy and Consumer Rights under the Digital Personal Data Protection Act, 2023. *Indian Journal of Cyber Law*, 6(1), 75–91.
26. Greenleaf, G. (2024). *Global Data Privacy Laws and Their Impact*. Oxford University Press.
27. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
28. United Nations Human Rights Council. (2023). *The Right to Privacy in the Digital Age*.
29. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
30. Ministry of Electronics and Information Technology. (2023). *DPDP Act Implementation Framework*.
31. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
32. Greenleaf, G. (2024). *Global Data Privacy Laws and Their Impact*.
33. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
34. MeitY. (2023). *Explanatory Framework for DPDP Act*.
35. OECD. (2024). *Consumer Policy and the Digital Transformation*.
36. Puttaswamy, K.S. (Retd.) v. Union of India, (2017) 10 SCC 1.
37. Bhandari, M. (2024). Data Privacy and Consumer Rights under the DPDP Act, 2023.
38. European Union. (2018). *General Data Protection Regulation (GDPR)*.
39. UNCTAD. (2024). *Digital Economy Report 2024*.
40. Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Harvard University Press.
41. OECD. (2024). *Consumer Policy and the Digital Transformation*. Paris: OECD Publishing.

∴