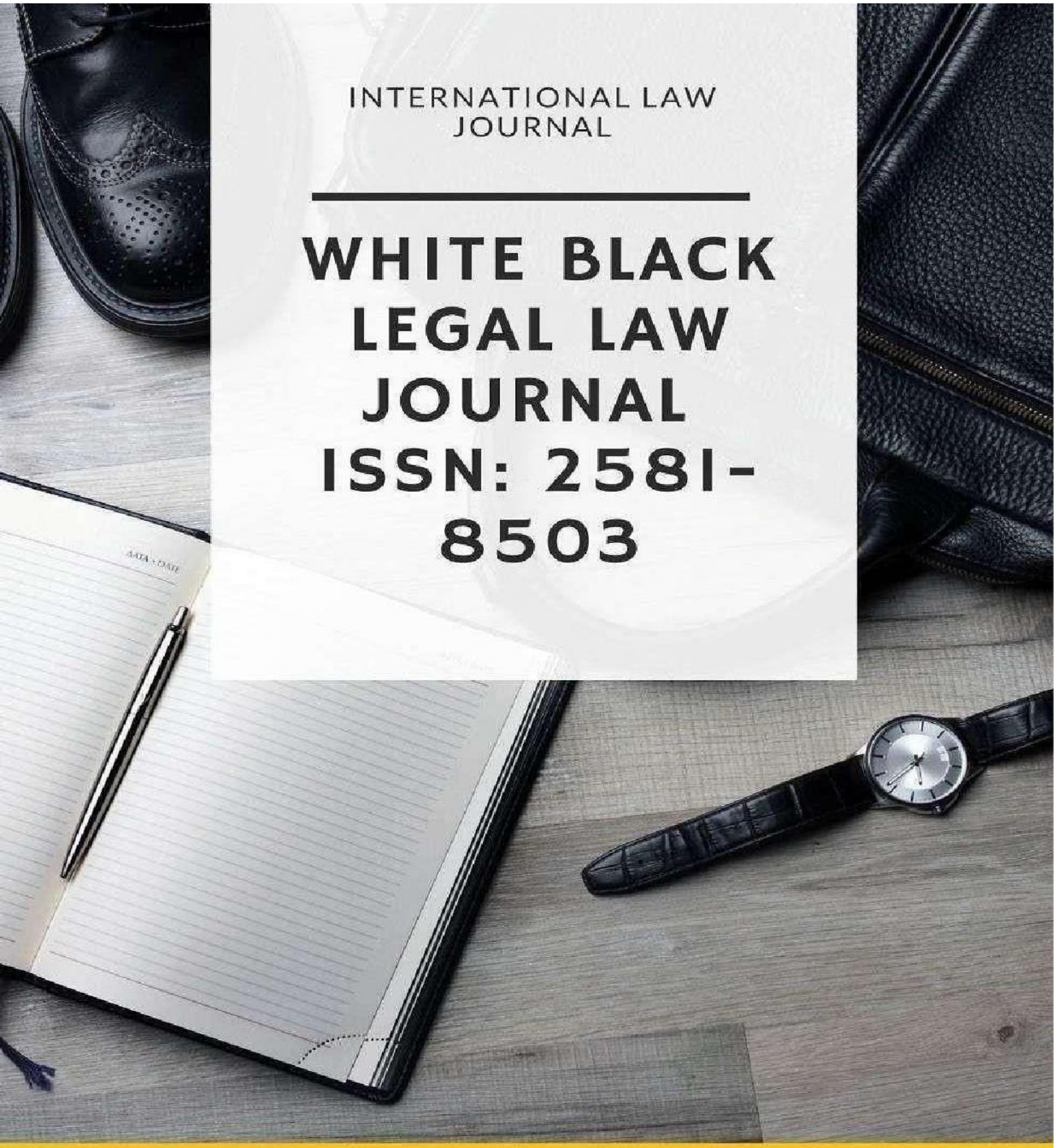

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Sep 2025 ISSN: 2581-8503

IMPLEMENTATION AND CHALLENGES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL LEGAL ANALYSIS

AUTHORED BY - DR SURENDRA KUMAR
Principal Mahavir Law College Kiran Path Mansarovar, Jaipur

Abstract

The Indian Constitution, which established that the right to privacy is a basic right, was the impetus for a dramatic reform in the data protection legislation of India. Taking into consideration the fast digitisation of data and the huge processing of data carried out by both public and commercial players, India went ahead and established the Digital Personal Data Protection Act, 2023 (DPDP Act) as the first complete legislation safeguarding personal data. Despite the fact that the Act represents a significant milestone in the legal framework, its effectiveness is contingent on the manner in which it is implemented, the ability of the institutions, and the degree to which it is effectively complied with. This study investigates the key challenges that are related with the implementation of the DPDP Act. These challenges include the limitations of the act in the workplace, consent fatigue, enforcement methods, state exclusions, cross-border data transfers, and the deficiency of knowledge among the general public. With a few brief analogies to the General Data Protection Regulation (GDPR) of the European Union (EU), the essay makes the argument that the DPDP Act runs the danger of becoming little more than a symbolic framework unless it overcomes the structural and operational faults involved. The purpose of this research is to give specific suggestions for improving the enforcement of the DPDP Act in accordance with the global digital world. These recommendations are prepared using doctrinal and comparative approaches.

Keywords: DPDP Act, Data Privacy, GDPR, Implementation Challenges, Data Protection Board.

1. Introduction

The proliferation of digital technology has resulted in the transformation of personal data into an invaluable asset for both public administration and the corporate sector organisations. Data collection, processing, and storage have become much less complicated in India as a result of initiatives such as Digital India, Aadhaar, the Unified Payments Interface (UPI), and large-scale e-governance systems. The digital revolution has brought forth new issues surrounding breaches of privacy and the unlawful use of personal data, despite the fact that it has led to successful and creative outcomes.[1]

The Indian Supreme Court established the right to privacy as a fundamental right in the case of ***Justice K.S. Puttaswamy v. Union of India***[2]. The need for strong data privacy laws in India was highlighted by this ruling. The Information Technology Act of 2000 was the principal law that ensured the right to data privacy before the DPDP Act was passed. But the data protection issues of today cannot be adequately addressed by this statute. This gap is meant to be closed by the Data Protection and Data Protection Act (DPDP Act), which establishes a structure for the protection of data and specifies the rights and responsibilities of data principals and data fiduciaries.[3]

However, the security of data cannot be guaranteed just by the implementation of regulations. Both the institutional structure and the methods that are used to carry out the implementation of the DPDP Act are the primary factors that determine how well it is enforced. The potential of the DPDP Act to provide adequate data protection is evaluated, taking into consideration the primary obstacles that stand in the way of its implementation.[4]

2. Evolution of Data Protection Law in India

India's journey towards a comprehensive data protection regime has evolved alongside the swift pace of the development of information technology and digital governance. The first comprehensive legislation was the Information Technology Act 2000 that was mainly concerned with cybercrimes, electronic commerce and electronic documents and digital

[1] "Ministry of Electronics and Information Technology (MeitY), Digital India, DIGITAL INDIA PROGRAMME, https://www.digitalindia.gov.in/ (last visited Aug. 30, 2025)."
[2] AIRONLINE 2018 SC 237
[3] Id.
[4] "Digital Personal Data Protection Act, 2023 of 2023, Act no. 22 0f 2023, Government of India [hereinafter referred as DPDP Act]; Information Technology Act, 2000 of 2000, No. 21 of 2000, INDIA CODE (2000) [hereinafter referred as IT Act]."

signatures being recognized in law. The Act was not specifically targeted at personal data, but did contain provisions relating to the security of data and unauthorised access to computer systems. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were a major step forward and include requirements for consent, privacy policies and reasonable security practices and procedures by corporate entities that handle sensitive personal data.

However, their scope is limited to private actors and they include no comprehensive provisions for the security of data or mechanisms for autonomous bodies to monitor and no enforceable rights of persons. The proliferation of digital services, e-commerce, social media, and governmental digital services have brought the shortcomings of the existing legal framework to light, in relation to problems with data use, hacks and mass surveillance.

In the landmark decision of Justice K.S. Puttaswamy (Retd.) v. Union of India, the highest court in India determined that data protection laws are legitimate since they are tied to the right to privacy in Article 21 of the Indian Constitution. Because of this, data protection regulations were passed and a committee headed by Justice B. N. Srikrishna was established. The committee's reports include A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) and a Personal Data Protection Bill draft.

After thorough examination and modification, the personal data Protection Bill, 2019 and the Data Protection Bill, 2021 were withdrawn. The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive digital personal data processing law, which has been passed by Parliament. The Act provides principles for lawful data processing, consent, individuals' rights, obligations of the data fiduciaries, cross-border transfers of data, and enforcement by the Data Protection Board of India is a significant move towards the rights-based approach to data protection in India.

3. Data Privacy Framework in India and European Union

The following rules make up India's data protection framework, which has developed over the years.

3.1 Information Technology Act, 2000 and SPDI Rules, 2011

The Information Technology Act, 2000, which focused primarily on cybercrimes and e-

commerce, was the foundation of security measures for data in India.[5] Section 43A of the Act established civil liability for inability to adhere to safety procedures, while Section 72A rendered it illegal to share personal information without consent.[6] In 2011, new regulations called the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were enacted. These rules expanded upon the existing regulations, provided a definition for sensitive personal data, and granted limited obligations to businesses.[7]

Nevertheless, the Information Technology Act did not provide sufficient rights, it did not have independent governmental monitoring, and it did not have effective enforcement mechanisms, which rendered it insufficient when taking into consideration the expansion of digital data storage and processing responsibilities.

3.2 Transition to the DPDP Act, 2023

As a result of the withdrawal of the Personal Data Protection Bill in 2019, India decided to implement a new and more simplified manner with the DPDP Act throughout the year 2023.[8] Only digital personal data is the subject of the Act, and its structure is based on permission, data primary rights, data fiduciary responsibilities, and severe consequences for breaches. The Act's emphasis is limited to digital personal data.[9] The DPDP Act, albeit adhering to international standards for data protection, presents significant difficulties in terms of its implementation due to the restricted scope and kind of organisational structure that it provides.

4. Digital Personal Data Protection (DPDP) Act, 2023

Information pertaining to a specific identifiable individual is known as personal data. Personal information is processed by both private companies and public agencies in order to facilitate the supply of products and services. Individual preferences may be better understood via data processing, which in turn can help with personalisation, targeted advertising, and suggestion development. Law enforcement agencies may also benefit from processing personal data. One of the most basic human rights is the right to privacy, which might be violated if processing is allowed to go amok. It might put people at risk of things like financial ruin, reputational

[5] IT Act, supra note 4.
[6] "IT Act §§ 43A, 72A."
[7] "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 of 2011, G.S.R. 313(E) [hereinafter referred as SPDI Rules]."
[8] "PRS Legislative Research, The Personal Data Protection Bill, 2019, PRS LEGISLATIVE RESEARCH (2019), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019."
[9] "DPDP Act §§ 5–16."

damage, and profiling, among other things.

There is no specific data protection legislation in India right now. The use of personally identifiable information is regulated under the Information Technology (IT) Act, 2000. Justice B. N. Srikrishna presided over a Committee of Experts on Data Protection that the federal government formed in 2017.[10] The purpose of forming the committee was to look at issues related to data protection in the nation. The Committee's report was due in July of 2018. The Personal Data Protection Bill, 2019 was introduced in Lok Sabha in December 2019 in accordance with the Committee's recommendations.[11] After reviewing the bill, a Joint Parliamentary Committee reported back in December 2021. In August 2022, the Bill was removed from consideration in Parliament. November 2022 saw the release of a draft bill for public review and comment. In August of 2023, lawmakers proposed the Digital Personal Data Protection Bill.[12]

Key Features

- **Applicability:** In India, the Bill governs the handling of digital personal data that is either (i) gathered online or (ii) digitised from offline sources. Data processing outside of India for the purpose of providing products or services in India is likewise subject to this regulation. Information pertaining to a specific identifiable individual is known as personal data. A processing operation is one that operates on digital personal data, either alone or in conjunction with other automated processes, and may be characterised as processing. This includes gathering, storing, using, and disseminating.
- **Consent:** The processing of personal data may only take place for legitimate purposes when the individual's permission has been obtained. Prior to requesting permission, notification must be provided. The specific personal information that will be gathered and why it will be processed should be included in the notification. You have the right to revoke your consent at any moment. For what are called "legitimate uses," prior consent is not needed in the following cases: (i) when a person willingly provides data for a specific purpose, (ii) when the government provides a benefit or service, (iii) in the event of a medical emergency, and (iv) when an individual is employed. The

[10] "Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021"
[11] "The Information Technology Act, 2000."
[12] The Digital Personal Data Protection Bill, 2019, as introduced in Lok Sabha.

approval of a parent or legal guardian will be required from anybody under the age of 18.

- **Transfer of personal data outside India:** Except for nations blacklisted by notice from the national government, the Bill permits transfer of personal data outside of India.
- **Exemptions:** In some situations, the data principal's rights and the data fiduciary's responsibilities (with the exception of data security) will not be applicable. Things like (i) investigating and preventing crimes and (ii) enforcing rights or claims that have been legally established fall under this category. Certain activities may be exempted from the application of the Bill by notice from the central government. Two examples are (i) processing for research, archiving, or statistical reasons and (ii) processing by government agencies to ensure public order and state security.
- **Data Protection Board of India:** "Data Protection Board of India" will be set up by the national government. The Board's primary responsibilities include: (i) ensuring compliance and enforcing fines; (ii) instructing data fiduciaries to respond appropriately to data breaches; and (iii) hearing complaints from those impacted. Membership on the board is appointed for a term of two years and is renewable if necessary. Such specifics as the procedure for selection and the total number of Board members will be dictated by the federal government. With respect to Board decisions, TDSAT shall have the last say.
- **Penalties:** Penalties for numerous violations are outlined in the Bill's schedule. For example, failing to perform commitments for minors may result in a penalty of up to (i) 200 crore rupees and (ii) 250 crore rupees for failing to take security measures to prevent data breaches. The Board will undertake an investigation and then decide on any necessary penalties.

5. Omission of the Right to Data Portability and the Right to be Forgotten: An Implementation Challenge under the DPDP Act, 2023

Right to be forgotten and data portability are not addressed in the bill. This protection was included in the 2018 draught bill and the 2019 draught bill that parliament considered. The 2019 Bill was examined by the Joint Parliamentary Committee, which suggested keeping these rights. Similarly, these rights are acknowledged by GDPR. A data protection legislation must have robust data principle rights, according to the Srikrishna Committee (2018). To ensure that people have agency over their data, these protections are founded on the principles of

accountability, openness, and autonomy.

Right to data portability: The right to data portability ensures that data proprietors may access and transfer their data in a generally used, machine-readable format from a data fiduciary for their own use. As a result, the data principle has more say over their information. It might make it easier to transfer data from one data custodian to another. The disclosure of the data fiduciary's trade secrets is one potential worry. The Srikrishna Committee (2018) had suggested that the right should be protected to the degree that the information may be provided without disclosing such trade secrets. According to the Joint Parliamentary Committee, technological feasibility is the sole valid reason to reject right data portability, not trade secrets.

Right to be forgotten: The "right to be forgotten" is a privacy measure that allows people to restrict how their personal information is shared online. According to the Srikrishna Committee (2018), the concept of the right to be forgotten seeks to impose memory constraints on an otherwise boundless digital realm. Nevertheless, it should be noted that this right could have to be balanced with other rights and interests, as pointed out by the Committee. This right, if used, might infringe upon the rights to free expression and information held by others. Some considerations that could determine its usefulness include the degree to which the protected information is sensitive, how relevant the information is to the general public, and the data principal's position in society.

6. Illustrative Case Studies on Data Protection under the DPDP Act and the GDPR

6.1 Justice K.S. Puttaswamy against the Union of India

An important landmark decision, this case upheld the right to privacy as a basic right under the Indian Constitution. This ruling established the framework for data protection in India by elucidating fundamental principles such as purpose restriction, consent, and the protection of data main rights. It provides the legal foundation for the DPDP Act.[13]

6.2 Aadhaar Case challenging Data Management by Unique Identification Authority of India (UIDAI)

The Aadhaar case investigated the security concerns regarding the sharing and utilisation of

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

personal data without consent by UIDAI biometric authentication services. The importance of data principals' rights in guaranteeing data privacy is underscored by the responsibilities of data fiduciaries, which include grievance redressal and consent management.[14]

6.3 Case - Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos

A major point of this ruling was its recognition of the right to be forgotten. This case highlights how the General Data Protection Regulation (GDPR) affords people more control over their personal data than the DPDP Act does, particularly in relation to access, deletion, and objection.[15]

6.4 Schrems II —Cross-border Data Flow

The EU–US Privacy Shield system was terminated by the Schrems II ruling due to its failure to safeguard personal data that was moved from the European Union to the United States. The ruling illustrates the stringent GDPR regulations that govern cross-border data transfers. The DPDP Act, in contrast, is primarily based on executive decisions and lacks regulatory provisions for trans-border data transfer.[16]

7. Key Implementation Challenges

Some of the difficulties in carrying out the DPDP Act are as follows: -

7.1 Data Protection Board and Institutional Capacity

The main entity tasked with carrying out the Data Protection Board of India's (DPB) mandate is the DPDP Act. In contrast to the independent regulatory agencies established by the GDPR, the executive choices are associated with the Board's selection process and management independence. Particularly in light of the processing of State data, this begs the concerns of autonomy, openness, and responsibility.

7.2 Complex Consent Prerequisites and Hidden Tricks

The DPDP Act places a premium on consent, but its effectiveness is diminished by complicated privacy disclosures, digital illiteracy, and hidden patterns. Because individuals often provide

[14] "Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018) 1 SCC 1 (Supreme Court of India 2018)."
[15] "Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C131/12, EU:C:2014:317."
[16] "Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18, EU:C:2020:559."

permission without completely comprehending the goal, it frequently turns into a formality instead of a thoughtful and reasoning choice.

7.3 Weak Enforcement and Penalty Execution

The DPDP Act imposes hefty penalties, but the lack of clarity around enforcement procedures, investigation powers, and administrative openness makes them effective deterrents. In contrast to the GDPR, India's regulatory framework is far from finished.

7.4 Cross-Border Data Transfers

Transferring data to countries that the government has designated as trustworthy is made possible under the DPDP Act. On the other hand, multinational corporations are confused by the absence of clear rules and safeguards, which might hurt India's standing in global data flows (unlike GDPR).

8. Conclusion

The Digital Personal Data Protection Act, 2023, has strengthened India's data protection system by upholding the constitutionally-guaranteed right to privacy. The Act establishes a fundamental legal framework for digital personal data; however, it will be ineffective unless it resolves common issues, including the autonomy of institutions, enforcement capacity, consent, and the regulation of state supervision.

The law may function primarily as a tool for providing guidelines for compliance for individuals and firms if it is not systematically enforced, rather than a framework to protect individuals' rights to secure digital personal data. The proper implementation of legislation depends on the Data Protection Board's autonomy, open and honest enforcement, and the growth of public understanding and competency with technology. In order for the DPDP Act to accomplish its goal of providing sufficient data privacy protection, ethical ideals and organisational dedication must be consistently put into practice.

References

1. Alessandro Acquisti, Curtis Taylor & Liad Wagman, The Economics of Privacy, 54 Journal of Economic Literature 442 (2016), https://pubs.aeaweb.org/doi/10.1257/jel.54.2.442.

2. Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18, EU:C:2020:559.
3. Digital Personal Data Protection Act, 2023 of 2023, Act no. 22 0f 2023, Government of India.
4. Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C-131/12, EU:C:2014:317.
5. Information Commissioner's Office, Penalty Notice to British Airways, Case Ref. COM0783542 (Oct. 16, 2020).
6. Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018) 1 SCC 1 (Supreme Court of India 2018).
7. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India 2017).
8. Ministry of Electronics and Information Technology (MeitY), Digital India, Digital India Programme, https://www.digitalindia.gov.in/ (last visited Aug. 30, 2025).
9. nformation Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 of 2011, G.S.R. 313(E).
10. PRS Legislative Research, The Personal Data Protection Bill, 2019, PRS Legislative Research (2019), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019