



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

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

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.

IMPACT OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL LEGAL ANALYSIS

AUTHORED BY - ASHIQ IMAM ALI

Assistant Professor

SMVEC Centre of Legal Education, Puducherry

ABSTRACT

The Digital Personal Data Protection Act, 2023 is an historic enactment aimed at regulating the processing of digital personal data in India while ensuring the privacy of individuals. It attempts to strike a balance between the protection of personal data and legitimate usage of information for governance, business and technology advancements. This paper looks into the various provisions of the Act and analyses their impact on individuals, businesses and authorities. It brings out the strengths of the legislation in terms of privacy and accountability among others while highlighting some of the weaknesses like wide-ranging government exemptions, compliance issues and others. In conclusion, the paper argues that the act is definitely a good step in the right direction but its success depends on its transparent implementation, judicial scrutiny and legal reforms.

Keywords: Digital Personal Data Protection Act, 2023, Privacy, Personal Data, Data Protection.

I. INTRODUCTION

Digital technologies have revolutionised the way personal data is collected, processed, stored, and shared. The collection of personal data takes place through online banking, ecommerce sites, health care applications, educational institutes, social networking sites, government websites, etc. Even as digitisation has brought about efficiencies and made things convenient, there are concerns related to misuse of personal information, identity theft, surveillance, profiling, and cyber crimes¹.

¹ Gupta Apar and Udbhav Tiwari, "The Future of Data Protection in India" 16 Indian Journal of Law and Technology 1 (2020).

Prior to 2023, India had no data protection law. Privacy matters in India had been dealt with using the Information Technology Act, 2000, and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. These provisions were felt to be inadequate in view of the fact that they covered only certain kinds of personal data and did not provide any rights².

The historic judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India³, in which it was held that privacy was a fundamental right under Article 21 of the Constitution, became the bedrock of privacy legislation. After a series of reports from various committees and a number of drafts, the (DPDP) Digital Personal Data Protection Act, 2023, was enacted by Parliament. The Act seeks to safeguard digital personal data while encouraging innovation and supporting India's digital economy.

II. OBJECTIVES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The primary objectives include:

- The main objectives are:
- To ensure the privacy of individuals;
- To regulate the digital processing of personal data;
- To facilitate the lawful processing through consent or legitimate uses;
- To hold Data Fiduciaries accountable;
- To bestow rights to Data Principals;
- To create a mechanism for grievances redressal; and
- To encourage responsible digital governance.

Unlike the General Data Protection Regulation (GDPR) EU, the DPDP Act employs a relatively simpler framework that is supposed to minimize compliance costs but still provide adequate protections.

² Ministry of Electronics and Information Technology, India's Digital Economy (Government of India, available at <https://www.meity.gov.in>)

³ (2017) 10 SCC 1.

III. KEY FEATURES OF THE ACT

3.1 Processing Through Consent

The DPDP Act recognizes consent as the key basis for processing personal data⁴. The consent shall be voluntary, explicit, informed, unambiguous, and freely revocable. This provision gives individuals the right to take charge of their personal data

3.2 Rights of Data Principals

The following are some of the key rights that have been provided under the Act⁵:

- Right to seek information.
- Right to correction.
- Right to data deletion.
- Right to lodge a complaint.
- Right to appoint a nominee.

These provisions enable individuals to exercise autonomy with respect to digital information.

3.3 Obligations of Data Fiduciaries

The organizations collecting personal information need to maintain⁶:

- Reasonable levels of security;
- Erasure of unnecessary information;
- Reporting of data breaches;
- Grievances redressal mechanisms; and
- Compliance with the direction issued by the government.
- Non-compliance leads to significant fines.

3.4 Data Protection Board

The Act sets up the Data Protection Board of India to deal with complaints, find non-compliance, and impose fines. As opposed to other foreign regulatory authorities, the Board mainly conducts itself in an adjudicatory capacity⁷.

⁴ Digital Personal Data Protection Act, 2023, s. 6

⁵ Digital Personal Data Protection Act, 2023, ss. 11–15

⁶ Digital Personal Data Protection Act, 2023, ss. 8–10

⁷ Digital Personal Data Protection Act, 2023, ss. 18–28

IV. POSITIVE CONSEQUENCES OF THE DPDP ACT

4.1 Privacy Protection

The Act implements constitutional privacy rights through statutory rights that allow individuals to request corrections or removal of inaccurate data⁸.

4.2 Increased Business Liability

Organisations cannot collect individuals' private data illegally. It will be necessary to improve internal control, protection from cyber-attacks and document everything.

4.3 Developing Digital Economy

Predictable regulation contributes to consumer trust in digital services. The trust can result in greater involvement in e-commerce, fintech, digital healthcare and online education.

4.4 Promoting Effective Cyber Security

Obligations concerning security encourage organisations to develop their technological background and incidents handling.

4.5 International Trust

Governments and multinational companies usually favour countries which have separate privacy laws. Thus, the DPDP Act might boost India's attractiveness for digital investments.

4.6 Effects on Business

Compliance requirements have become much more stringent. Big organizations will have to rework their privacy policies, consent mechanism, staff training programs, contract agreements with vendors, and cybersecurity protocols. For start-ups, the cost of compliance might be relatively high due to a lack of funds.

On the other hand, increased consumer confidence may lead to business benefits in the long run⁹. Those companies that work in the field of artificial intelligence, cloud computing, fintech, healthtech, and digital marketing in particular will find themselves facing many regulatory changes.

⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

⁹ OECD, The OECD Privacy Framework (2013)

4.7 Effects on Government

Another hotly-debated issue is about governmental exemptions. The central government can exempt certain departments from some provisions in special cases like sovereignty, security, public order, and prevention of offenses.

Opponents point out that too many exemptions may make privacy protection weaker and lessen government's accountability. Proponents believe that exemptions are needed for national security and proper governance. It remains to be seen whether these provisions will be constitutional.

V. NEGATIVE EFFECT OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 represents an important development towards the protection of personal data in India; however, many provisions of the Act have faced criticism from various legal experts, privacy activists, and other stakeholders due to their implications for the constitutionality and efficiency of the Act.

5.1 Wide Exemptions for the Government

The most controversial aspect of the Act is related to the ability of the Central Government to exempt certain government authorities from the scope of application of many provisions of the Act on the grounds of national security, sovereignty, public order, and prevention of offences¹⁰. Although these purposes are justified, the formulation of this provision is very wide and leaves the decision-making process in the hands of the executive. It is argued that such wide exemptions could undermine the constitutional right to privacy recognized by the Supreme Court of India in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India.

5.2 Higher Compliance Costs

Under this Act, Data Fiduciaries have to put up measures of data security, grievance redressals, report data breaches and keep their compliance records. Although such duties help protect data privacy, they come at a considerable cost.

While large multinational corporations can adjust to these compliance obligations quite easily, start-ups, small-scale businesses, colleges, hospitals, and NGOs might find it hard to meet these

¹⁰ Digital Personal Data Protection Act, 2023, s. 17

compliance requirements. This could mean higher costs of compliance, which could hinder innovations and pose obstacles in front of new businesses¹¹.

5.3 Lack of Privacy Rights

In comparison to other international privacy laws like GDPR by the EU, the DPDP Act lacks certain rights of an individual. These rights include data portability, right to objection, and protection from automated decision making¹².

With the rising use of artificial intelligence and algorithmic decision-making systems, the lack of such rights may lower protection levels of the citizens of India.

5.4 Restricted Independence of the Data Protection Board

India's Data Protection Board has been set up as the principal enforcement agency for the Act. But concerns have been expressed about the Board's institutional independence since the Central Government has a substantial say in the makeup of the Board and its functions.

An efficient regulation agency must be independent while investigating cases against both private parties and government departments. The involvement of executives may undermine public faith in the independence of the Board.

5.5 Uncertainty Owing to Rule Making Power

Several critical issues about the operation of the Act have been left to be sorted out through future rules to be made by the Central Government. Issues concerning consent notices, breach notifications, and duties of Significant Data Fiduciaries need to be clarified.

5.6 Challenges to Cross-Border Business Operations

According to the Act, there can be cross-border transfers of personal data only to nations which are not limited by the Central Government¹³. Though this gives regulatory flexibility, businesses that operate across borders will be in for tough times if limitations are placed on this matter in the future.

There is a possibility that businesses involved in cloud computing, outsourcing, fintech, and other multinational digital services will have to make changes to their methods of handling data

¹¹ NASSCOM, Data Protection and Business Readiness Report (2024)

¹² Gautam Bhatia, Privacy and the Indian Constitution (Oxford University Press, 2019)

¹³ DPDP Act, 2023, s. 16

based on future government decisions¹⁴.

5.7 Burden on Digital Innovation

The stringent nature of compliance requirements can pose an obstacle in the way of innovations of startups since developers in the areas of artificial intelligence, machine learning, health technology, and data analytics depend on huge amounts of data to create innovations¹⁵.

It will be difficult for smaller innovators to compete with big corporations that have legal and compliance departments when the process becomes too complicated.

5.8 Public Awareness and Digital Literacy

The success of any privacy law hinges on the ability of people to know their rights. There are millions of Internet users in India who do not have a clue about the concepts like consent management, revocation of consent, grievance redressal, and erasure of data.

5.9 The Possibility of Regulatory Overlap

While DPDP is a general act on privacy protection, other sectoral laws are in place regarding banking, telecommunications, healthcare, insurance, and finance. The multiplicity of legal systems might lead to confusion about who is responsible for what and where the jurisdiction lies.

Organizations that work in different sectors will face problems of overlapping regulation and increased legal burden.

5.10 Privacy versus Economic Development

The law tries to find a balance between protection of privacy and development of the economy and technology. Maintaining such a balance will continue to be difficult, because too much regulation will scare off investors, while too little will leave people unprotected from privacy breaches. Interpretation by courts and future legislation amendments will have to help keep this balance¹⁶.

¹⁴ Ministry of Electronics and Information Technology, Draft DPDP Rules, 2025.

¹⁵ OECD, *Artificial Intelligence Principles* (2019).

¹⁶ Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

VI. COMPARISON WITH GDPR

Despite being drawn from international principles on privacy, there are clear distinctions between the Indian legislative regime and GDPR. The GDPR has more expansive rights like the right to portability and right to object processing. It provides for an independent supervisory authority in each member state¹⁷.

On the other hand, the DPDP Act takes a more flexible compliance approach suited to the needs of a developing digital economy in India. The Indian legislature is inclined towards a simpler administrative regime rather than complex regulation¹⁸.

7. RECOMMENDATIONS

The efficacy of the DPDP Act can be improved through¹⁹:

- institutionalizing the independence of the Data Protection Board;
- clarity on governmental exceptions;
- public education campaigns;
- compliance guidelines;
- privacy-by-design approach;
- digital literacy;
- sector-specific compliance regimes;
- judicial oversight.

CONCLUSION

The Digital Personal Data Protection Act, 2023 is one of the biggest legal reforms in India's digital governance regime. It captures the constitutional spirit of privacy protection while also aiding innovation in the economy.

Despite the presence of many forward-looking provisions in the act, its successful implementation is going to be the key to its success. Regulatory transparency, institutional

¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), arts. 15–22

¹⁸ Graham Greenleaf, Global Data Privacy Laws 2024: With All Its Weaknesses, 80% of the Globe is Covered by Data Privacy Laws, Privacy Laws & Business International Report (2024).

¹⁹ United Nations Conference on Trade and Development (UNCTAD), Data Protection and Privacy Laws Globally (2024).

independence, corporate compliance, and judicial oversight will play a crucial role in accomplishing the aims of the Act.

In light of the continuous growth of India's digital economy, the DPDP Act will continue to influence the future relationship among technology, privacy, and governance in India. Thus, the review and evolution of legislation in this regard will prove to be vital.

