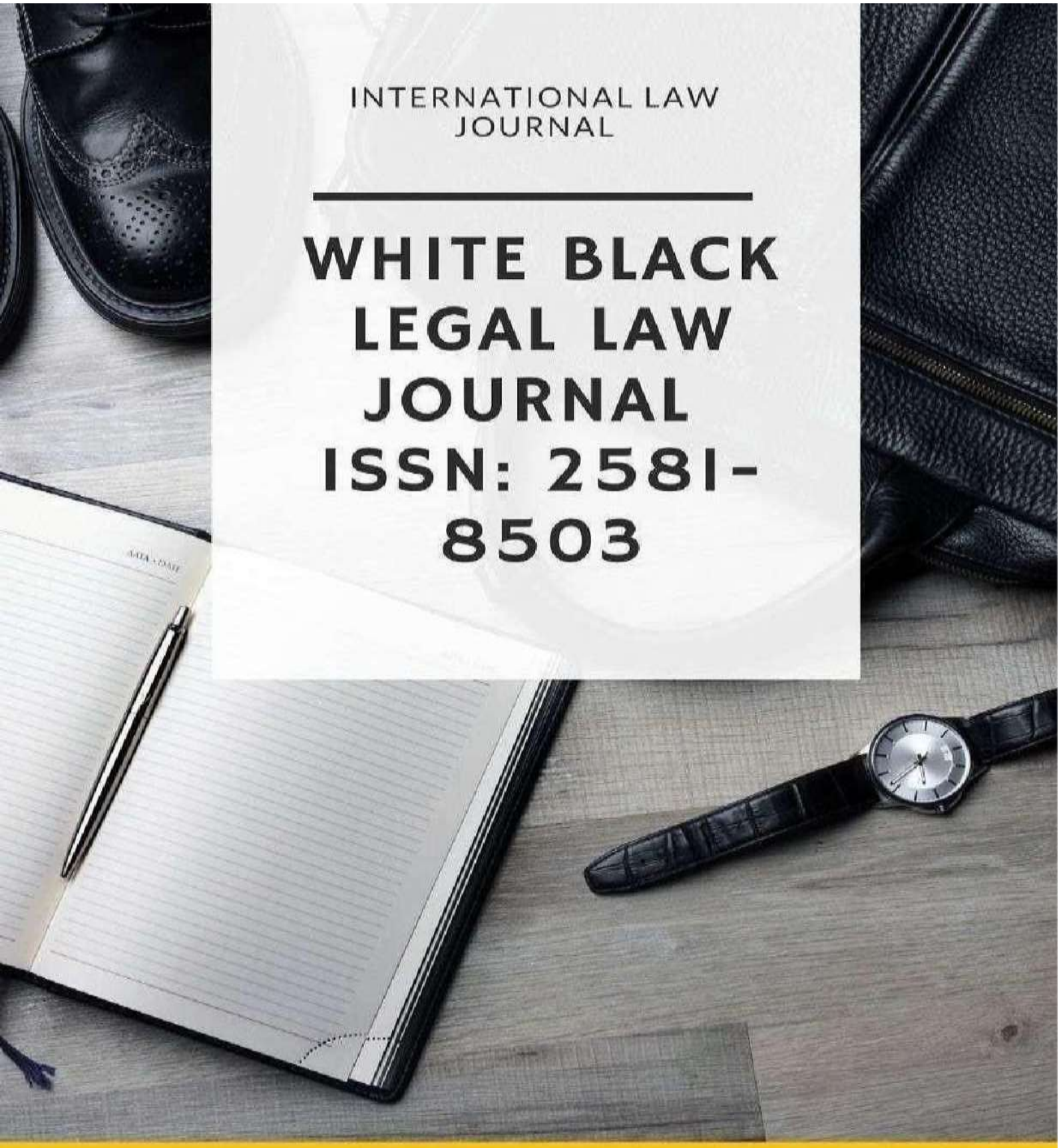

INTERNATIONAL LAW JOURNAL

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

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

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

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

DATA PRIVACY IN INDIA POST-DPDP ACT, 2023: A CRITICAL APPRAISAL

AUTHORED BY - VIKAS
Pursuing PH.D
Singhania University, Pacheri Bari, Jhunjhunu Rajasthan

Abstract

The enactment of the Digital Personal Data Protection Act, 2023 marks a watershed moment in India's journey toward establishing a robust data privacy regime. Enacted in response to the landmark Supreme Court judgment in *Justice K.S. Puttaswamy v Union of India*, which recognised privacy as a fundamental right, the DPDP Act aims to create a legal framework for the protection of personal data in the digital era. This paper critically examines the key features of the Act, including consent architecture, data fiduciary obligations, cross-border data flow, and enforcement mechanisms. It evaluates the Act's adequacy in balancing individual privacy rights with the legitimate interests of the state and private entities. By comparing global privacy standards, especially the European Union's GDPR, the study analyses whether the DPDP Act lives up to the constitutional promises and international expectations. The paper also identifies gaps in accountability, data subject rights, and institutional independence, raising pertinent questions about the Act's capacity to effectively safeguard citizens' digital autonomy. Through doctrinal and comparative analysis, this research seeks to highlight the strengths and weaknesses of the new law, offering recommendations for future reform and implementation.

Keywords

Data Protection, Digital Personal Data Protection Act 2023, Privacy Rights, Consent, Data Fiduciary, Cross-Border Data Transfer, Surveillance, Fundamental Rights, GDPR, Legal Framework, Accountability, Data Governance

Literature Review

The evolution of data privacy discourse in India has largely been shaped by judicial intervention and the absence of a dedicated statutory framework until recently. The Supreme Court's landmark verdict in *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) provided

the constitutional foundation for recognising privacy as a fundamental right, laying the groundwork for subsequent legislative developments.

Several scholars have examined the shortcomings of India's previous data regulation regime, particularly the Information Technology Act, 2000 and its associated rules. Rahul Matthan (2017) argues that the IT Act failed to adequately address concerns related to consent, data minimisation, and accountability, especially in the age of algorithmic profiling and mass data collection.[1]

The Justice B.N. Srikrishna Committee Report (2018) was a pivotal contribution to the academic and policy discourse. The Committee proposed a rights-based framework and recommended the establishment of a Data Protection Authority (DPA) to ensure independent regulation. Scholars such as Malavika Raghavan and Sunil Abraham have praised the report's alignment with global best practices but also cautioned against potential state overreach and surveillance.

In comparison, the European Union's General Data Protection Regulation (GDPR) has often been viewed as the gold standard for data protection globally. Academics like Graham Greenleaf and Lee Bygrave have explored how GDPR emphasises individual rights, purpose limitation, and regulatory independence.[2] Comparative analyses highlight the importance of ensuring that data protection laws do not merely exist in form, but function in a manner that respects user autonomy and legal transparency.

With the introduction of the Digital Personal Data Protection Act, 2023, early academic responses have been mixed. While the Act has been applauded for institutionalising consent and creating clearer obligations for data fiduciaries, concerns remain about the dilution of the DPA's independence, the wide exemptions granted to the state, and the lack of clarity on algorithmic accountability. These debates form the basis for a critical appraisal of the Act within this research.

[1] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection' (2017) *The Takshashila Institution*
[2] Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 *Privacy Laws & Business International Report* 1.

Research Methodology

This research adopts a **doctrinal and analytical** methodology, focusing on the critical examination of statutory texts, judicial pronouncements, and secondary academic literature to evaluate the effectiveness and limitations of the Digital Personal Data Protection Act, 2023. The study is grounded in legal interpretation, comparative analysis, and policy review.

Primary sources include the DPDP Act, 2023 itself, constitutional provisions such as Article 21 of the Indian Constitution (Right to Life and Personal Liberty), and landmark judgments including *Justice K.S. Puttaswamy (Retd.) v Union of India*. These materials form the foundation for assessing the Act's alignment with constitutional values and human rights principles.

Secondary sources comprise scholarly articles, committee reports (notably the Justice Srikrishna Committee Report), journal publications, and expert opinions from legal think tanks. Comparative references to international legal instruments such as the European Union's GDPR are used to identify global best practices and benchmark the Indian framework accordingly.

The research also uses a **comparative legal approach** to contrast the Indian regime with global standards of data protection. This helps in identifying both the innovations and gaps in India's legislation.

The objective is not only to evaluate the legal text but also to understand its broader implications for digital rights, privacy protection, and administrative accountability. No empirical data collection has been conducted; the study is qualitative in nature and relies on legal reasoning and critical evaluation.

Hypothesis

The research is based on the hypothesis that **while the Digital Personal Data Protection Act, 2023 marks a significant legislative advancement in India's data governance framework, it falls short in fully safeguarding individual privacy due to inadequate regulatory independence, broad state exemptions, and weak enforcement mechanisms**.

This hypothesis will be tested by critically examining the structure, provisions, and implementation potential of the DPDP Act in light of constitutional principles, international best practices (such as GDPR), and concerns raised by legal scholars and civil society organisations. The research anticipates that the Act's promise of protecting digital autonomy may be undermined by its compromises on accountability and oversight.

Introduction

In the digital age, data has emerged as the most valuable asset, often termed the "new oil." With growing internet penetration, e-governance, and digital transactions, the collection, processing, and storage of personal data have expanded exponentially in India. This surge has triggered serious concerns about how individuals' personal information is used, secured, and protected from misuse, prompting demands for a dedicated legal framework for data privacy.

The recognition of the right to privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v Union of India* was a constitutional turning point.[3] The judgment emphasised the need for a robust data protection regime that respects informational autonomy, consent, and proportionality. This judicial pronouncement laid the foundation for legislative efforts that culminated in the enactment of the **Digital Personal Data Protection Act, 2023**.

The DPDP Act aims to create a rights-based data protection framework, focusing on informed consent, purpose limitation, and accountability of data fiduciaries. It introduces key concepts such as "data principal," "data fiduciary," "consent manager," and delineates obligations for both private and public entities. However, critics argue that the Act provides the state with sweeping exemptions, lacks an independent data protection authority, and omits several safeguards recommended in the earlier Srikrishna Committee report.[4]

While the legislation is a much-needed step forward, its effectiveness in practice depends on institutional mechanisms, enforcement capacity, and the government's willingness to uphold individual privacy even when it conflicts with state interests. As such, the Act warrants a thorough critical appraisal.

[3] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
[4] Vrinda Bhandari and Amber Sinha, 'The DPDP Bill 2022: Disappointments and Discrepancies' (2022) *The Leaflet*

This paper seeks to evaluate whether the DPDP Act, 2023 effectively fulfils its stated objectives of protecting digital personal data and empowering citizens, or whether it suffers from structural and ethical shortcomings that may dilute its potential.

1. Legal Framework and Constitutional Alignment

The **Digital Personal Data Protection (DPDP) Act, 2023**, is India's first dedicated legislation focusing exclusively on digital personal data. It draws heavily from global data protection principles like those in the **General Data Protection Regulation (GDPR)** but also reflects India's constitutional jurisprudence post-*Justice K.S. Puttaswamy v. Union of India*. In that case, the Supreme Court affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution.[5]

However, some critics argue that despite good intentions, the Act's provision enabling the Central Government to exempt any instrumentality of the state from its application weakens the law's credibility and undermines constitutional privacy protections. The discretionary nature of Section 17 of the Act raises serious questions regarding state surveillance and overreach.[6]

Moreover, the Act's avoidance of data localization—by allowing cross-border data flows to "notified countries"—has gained mixed reactions. While it promotes ease of doing business, it opens the door to potential misuse if adequate protections are not ensured in recipient jurisdictions.[7]

2. Rights of Individuals vs. Responsibilities of Fiduciaries

The DPDP Act enshrines specific rights for data principals (individuals), including the **right to information, correction, erasure**, and **grievance redressal**. These rights empower individuals to maintain control over their personal data. Notably, the Act introduces a user-friendly framework using plain-language "consent forms" and an accessible complaint mechanism through the **Data Protection Board of India (DPBI)**.[8]

[5] Digital Personal Data Protection Act 2023, s 17
[6] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[7] Smriti Parsheera, 'India's Data Protection Law: A Missed Opportunity for Stronger Privacy' (2023) 18(4) NUJS L Rev 213
[8] Digital Personal Data Protection Act 2023, s 11 (Rights of Data Principal).

On the flip side, data fiduciaries are required to implement stringent security safeguards, conduct Data Protection Impact Assessments (DPIAs), and appoint a **Data Protection Officer (DPO)** in certain cases. While this aligns with global best practices, micro and small enterprises have raised concerns about the economic burden of compliance. The exemption for startups and certain small businesses, while providing relief, also poses a risk of creating uneven standards of accountability.[9]

The Act also lacks clarity on **automated decision-making**, a crucial gap in the age of algorithmic profiling and AI, which directly affects data subjects' rights without clear recourse.

3. Oversight and Enforcement

The **Data Protection Board of India (DPBI)** is tasked with enforcing compliance and adjudicating violations under the Act. Unlike the GDPR's robust and independent supervisory authorities, the DPBI is designed as an administrative body under the central government, with its members appointed by the Union. This raises concerns about independence and the risk of politicization of oversight functions.

The penalties prescribed for non-compliance—ranging from ₹10,000 to ₹250 crore—may be significant on paper, but the effectiveness of enforcement will depend on the DPBI's operational capacity, resources, and neutrality.

Another concern is the **lack of judicial review** for many of the Board's decisions. Critics argue this could result in unchecked administrative actions and dilute the accountability framework required in a rights-based data governance system.

Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023 marks a significant step toward safeguarding data privacy in India by establishing a legal framework for personal data processing, defining individual rights, and imposing obligations on data fiduciaries. However, while the Act addresses long-standing gaps in India's data protection regime, it also presents several challenges and ambiguities that warrant critical appraisal.

[9] Data Protection Board of India, 'FAQs on Compliance Requirements' (DPBI, 2024)

On the positive side, the DPDP Act introduces key principles such as consent-based data processing, data minimization, and accountability mechanisms. It also empowers individuals with rights like the right to access, correct, and erase their data, aligning India's privacy framework with global standards like the GDPR. The establishment of a Data Protection Board (DPB) as an adjudicatory body is another progressive move.

Yet, the Act has notable shortcomings. Exemptions granted to government agencies on vague grounds of "national security" and "public order" raise concerns about potential overreach and dilution of privacy rights. The lack of an independent appellate tribunal and the absence of detailed provisions on cross-border data transfers further weaken its effectiveness. Additionally, the Act's silence on non-personal data and its limited emphasis on harm mitigation leave gaps in comprehensive data governance.

In conclusion, while the DPDP Act, 2023 is a commendable effort toward strengthening data privacy in India, its implementation will determine its true efficacy. Future amendments should focus on enhancing transparency, minimizing government exemptions, and ensuring robust enforcement to strike a balance between privacy rights and digital growth. Until then, India's data protection landscape remains a work in progress, requiring continuous scrutiny and refinement.