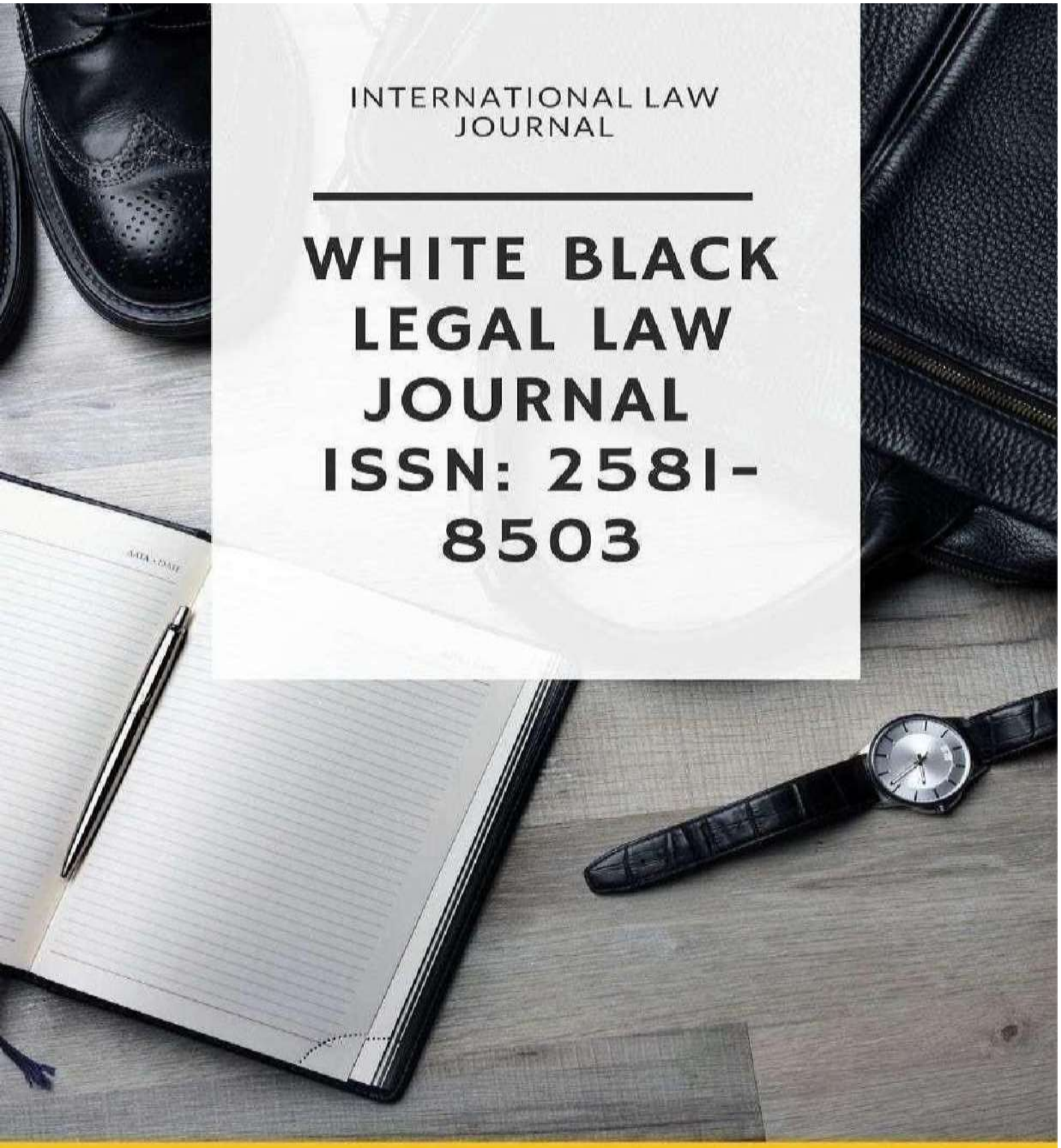

INTERNATIONAL LAW JOURNAL

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 PROTECTION IN INDIA: NAVIGATING THE LEGAL LANDSCAPE UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY: VASUDHA SAINI
Faculty of Law, University of Delhi

ABSTRACT

The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) enshrined privacy as a fundamental right, spurring India to overhaul its data protection framework. The Digital Personal Data Protection Act, 2023 (DPDP Act) emerged as a cornerstone of this transformation, aiming to regulate personal data processing in India's rapidly expanding digital economy. This paper critically examines the DPDP Act, its alignment with global standards, the 2025 draft rules, and the institutional mechanisms for enforcement. It explores judicial trends, compliance challenges, and the delicate balance between individual rights, state interests, and economic growth. Drawing comparisons with frameworks like the EU's General Data Protection Regulation (GDPR), the study highlights gaps in India's regime and proposes reforms to foster a transparent, rights-centric data governance model. The paper concludes that the DPDP Act's success depends on robust rulemaking, independent oversight, and a commitment to constitutional principles.

INTRODUCTION

India's digital economy is on a meteoric rise, with projections estimating a $1 trillion valuation by 2030, fueled by over 900 million internet users and widespread adoption of digital payments.[1] This growth has unleashed an unprecedented volume of personal data, raising urgent questions about privacy and security. The Supreme Court's 2017 ruling in *Justice K.S. Puttaswamy v. Union of India* declared the right to privacy a fundamental right under Article 21 of the Constitution, laying the constitutional groundwork for a modern data protection regime.[2] The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step forward, replacing the outdated provisions of Section 43A of the Information Technology Act, 2000 and the Sensitive Personal Data or Information (SPDI) Rules, 2011.[3]

This paper delves into the DPDP Act's framework, its operationalization through the 2025 draft rules, and the institutional structures designed to enforce it. It analyzes judicial and regulatory developments, compares India's approach with global standards, and identifies challenges such as state surveillance and compliance burdens. By proposing actionable reforms, the paper seeks to chart a path for a data protection regime that balances individual rights with India's ambitions as a global digital hub.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A NEW ERA

Historical Context

The DPDP Act, enacted in August 2023, emerged from years of deliberation, including the 2018 Justice Srikrishna Committee Report and earlier drafts like the Personal Data Protection Bill, 2019.[4] The *Puttaswamy* judgment catalyzed these efforts, emphasizing the need for a law to protect informational privacy in an increasingly data-driven society. The Act aims to regulate the processing of digital personal data while fostering innovation and economic growth.

Key Features

The DPDP Act adopts a principle-based approach, focusing on consent, transparency, and accountability:

- **Core Definitions**:
  - **Personal Data**: Any information that can identify an individual, whether directly or indirectly.[5]
  - **Data Fiduciary**: Entities or individuals determining the purpose and means of data processing, akin to a "data controller" in global frameworks.[6]
  - **Data Principal**: The individual whose data is processed.[7]
  - **Consent**: Must be free, informed, specific, and unambiguous, requiring an affirmative action from the Data Principal.[8]
- **Rights of Data Principals**:
  - Access to details about how their data is processed.
  - Correction, updating, or deletion of personal data.
  - Nomination of successors to manage data in case of incapacity or death.
  - Access to grievance redressal mechanisms through Data Fiduciaries or the

Data Protection Board.[9]

- **Obligations of Data Fiduciaries**:
  - Secure verifiable consent before processing data.
  - Implement robust security measures to protect data.
  - Report data breaches to the Data Protection Board and affected individuals promptly.
  - Appoint a Data Protection Officer for entities handling significant data volumes.[10]
- **Penalties**: Violations attract fines up to ₹250 crore per instance, with a tiered structure based on the breach's severity.[11]

Scope and Exemptions

The DPDP Act applies to all digital personal data processed in India and by foreign entities targeting Indian residents. However, it includes broad exemptions for state agencies, allowing data processing for national security, law enforcement, or public order without stringent oversight.[12] These exemptions have sparked concerns about potential misuse, given India's history of surveillance programs like the Central Monitoring System.[13]

THE 2025 DRAFT RULES: BRINGING THE ACT TO LIFE

In January 2025, the Ministry of Electronics and Information Technology (MeitY) released draft rules to operationalize the DPDP Act. These rules provide clarity on implementation and address practical challenges:

1. **Cross-Border Data Transfers**:
   - The Act permits data transfers abroad but allows the government to restrict transfers to jurisdictions on a "negative list" based on inadequate data protection standards.[14] The draft rules outline criteria such as reciprocity and cybersecurity frameworks, moving away from earlier proposals for mandatory data localisation.
2. **Protection for Minors**:
   - Processing data of individuals under 18 requires verifiable parental consent, facilitated through government-issued IDs or digital tokens.[15]
   - The rules mandate simplified privacy notices and age-verification mechanisms to ensure accessibility for minors.

3. **Multilingual Accessibility**:
    - To address India's linguistic diversity, consent notices and privacy policies must be available in all 22 official languages listed in the Eighth Schedule of the Constitution.[16]
4. **Data Breach Notifications**:
    - Data Fiduciaries must report breaches to the Data Protection Board and affected individuals within 72 hours, aligning with global best practices.[17]
    - The rules specify standardized reporting formats and require incident logs for audits.
5. **Significant Data Fiduciaries**:
    - Entities processing large volumes of sensitive data (e.g., health or financial records) face stricter obligations, including mandatory audits and data protection impact assessments.[18]

While the draft rules enhance the Act's practicality, their complexity may challenge smaller organizations, necessitating simplified compliance pathways.

THE DATA PROTECTION BOARD: INSTITUTIONAL BACKBONE

Role and Structure

The DPDP Act establishes the Data Protection Board of India (DPBI) as an independent adjudicatory body tasked with:

- Investigating data breaches and imposing penalties.
- Resolving grievances from Data Principals.
- Issuing compliance directives to Data Fiduciaries.[19]

The Board, appointed by the central government, includes experts in law, technology, and data governance. The Union Budget 2024–25 allocated ₹2 crore for its establishment, but as of June 2025, the DPBI remains non-functional, delaying enforcement.[20]

Concerns Over Independence

The DPBI's placement under executive control raises questions about its impartiality, unlike GDPR's fully independent Data Protection Authorities.[21] Critics argue that government-appointed members may face pressure in cases involving state agencies, undermining public trust. Models like the UK's Information Commissioner's Office, with statutory independence,

offer a blueprint for reform.[22]

Temporary Enforcement Measures

In the absence of the DPBI, sectoral regulators have stepped in. The Reserve Bank of India's Online Dispute Resolution (ODR) framework for digital payments and the Securities and Exchange Board of India's cybersecurity guidelines for market intermediaries complement the DPDP Act's objectives.[23] However, this fragmented approach risks inconsistent enforcement.

JUDICIAL AND REGULATORY DEVELOPMENTS

Key Court Rulings

The *Puttaswamy* judgment remains the bedrock of India's privacy jurisprudence, emphasizing proportionality in state actions affecting privacy.[24] Recent cases further define the landscape:

- **Meta–WhatsApp Case (2024–2025)**: In October 2024, the Competition Commission of India (CCI) imposed a ₹25.4 million fine on Meta for anti-competitive data-sharing practices between WhatsApp and Facebook.[25] The National Company Law Appellate Tribunal stayed the order in January 2025, pending appeal.[26] This case highlights the intersection of competition law and data privacy, underscoring the need for harmonized regulation.
- **Aadhaar Challenges (2024)**: Ongoing litigation questions the mandatory linkage of Aadhaar for digital services, with courts reinforcing the need for informed consent and minimal data collection.[27] These rulings strengthen the DPDP Act's consent framework but challenge its state exemptions.

Regulatory Initiatives

- **RBI's ODR Framework (2024)**: Mandates automated grievance platforms for digital payment disputes, aligning with the DPDP Act's redressal goals.[28]
- **SEBI's Cybersecurity Guidelines (2024)**: Require market intermediaries to adopt data protection measures, complementing the Act's security obligations.[29]
- **MeitY's AI Ethics Principles (2024)**: Address privacy risks in AI systems, urging alignment with the DPDP Act.[30]

These developments signal a multi-regulatory approach, but overlapping jurisdictions may lead to confusion and inefficiencies.

GLOBAL COMPARISONS: DPDP ACT IN CONTEXT

The DPDP Act draws inspiration from global frameworks like GDPR but reflects India's unique priorities:

Feature	DPDP Act	GDPR
Consent Age for Minors	18 (requires parental consent)	13–16 (varies by Member State)
Cross-Border Transfers	Permitted with negative list restrictions	Limited to 'adequate' jurisdictions or with safeguards
State Exemptions	Broad, covering national security and law enforcement	Narrow, subject to judicial oversight
Regulator Independence	DPBI under executive oversight	Independent Data Protection Authorities
Penalties	Up to ₹250 crore per violation	Up to €20 million or 4% of global turnover

Shared Principles

- **Consent and Rights**: Both frameworks emphasize informed consent and grant rights like access, correction, and erasure. The DPDP Act's grievance redressal aligns with GDPR's complaint mechanisms.[31]
- **Breach Notification**: The 72-hour reporting requirement mirrors GDPR's timeline.[32]
- **Accountability**: Both mandate security measures and impact assessments for high-risk data processing.

Key Differences

- **State Powers**: The DPDP Act's broad exemptions for state agencies contrast with GDPR's stricter oversight, raising concerns about unchecked surveillance.[33]
- **Regulatory Autonomy**: GDPR's independent authorities contrast with the DPBI's executive control, impacting enforcement credibility.[34]

- **Data Transfers**: The DPDP Act's negative list is less restrictive than GDPR's adequacy framework, potentially easing global data flows but risking weaker protections.[35]

Insights from Other Jurisdictions

- **Singapore's PDPA**: Offers flexible compliance for SMEs, a model for easing India's startup burdens.[36]
- **Brazil's LGPD**: Emphasizes judicial oversight, suggesting a path for strengthening the DPBI.[37]
- **China's PIPL**: Prioritizes state control but imposes strict localisation, contrasting with India's liberal transfer policy.[38]

These comparisons highlight opportunities for India to refine its framework while leveraging its strengths as a data processing hub.

CHALLENGES AND PATHS FORWARD

Key Obstacles

1. **Lack of Sectoral Guidance**: The DPDP Act's broad principles lack tailored guidelines for sectors like healthcare and fintech, risking uneven compliance.[39]
2. **State Surveillance**: Broad exemptions for national security may violate *Puttaswamy*'s proportionality principle, enabling unchecked data access.[40]
3. **Compliance Costs**: Small businesses face high costs for multilingual notices and audits, potentially stifling innovation.[41]
4. **Digital Divide**: With only 26% internet penetration in rural India, access to data protection rights remains unequal.[42]
5. **Delayed Enforcement**: The DPBI's non-operational status delays accountability and erodes trust.[43]

Opportunities for Growth

1. **Technological Innovation**: AI-driven consent management and blockchain-based secure data sharing can streamline compliance.[44]
2. **Global Leadership**: A robust DPDP regime could position India as a trusted data processing destination, boosting foreign investment.[45]
3. **Judicial Oversight**: Courts can ensure proportionality in state data access,

reinforcing constitutional protections.[46]

Recommendations

1. **Strengthen DPBI Autonomy**: Grant statutory independence to the DPBI, with parliamentary oversight to ensure impartiality.
2. **Issue Sectoral Guidelines**: Develop codes of practice for key industries to clarify compliance requirements.
3. **Limit State Exemptions**: Introduce judicial review for state data access to align with constitutional standards.
4. **Support SMEs**: Provide compliance subsidies and digital tools to ease burdens on startups.
5. **Promote Digital Literacy**: Launch campaigns in regional languages to educate citizens about data rights.
6. **Regular Review**: Establish a five-year review cycle to adapt the DPDP Act to technological and societal shifts.

CONCLUSION

The Digital Personal Data Protection Act, 2023, heralds a new chapter in India's data governance journey, rooted in the constitutional recognition of privacy. By emphasizing consent, transparency, and accountability, the Act aligns with global standards while addressing India's unique digital landscape. The 2025 draft rules provide operational clarity, but challenges like state exemptions, compliance costs, and the DPBI's delayed operationalization persist. Comparative insights from GDPR, Singapore's PDPA, and Brazil's LGPD highlight areas for refinement, particularly in regulatory independence and sectoral clarity.

To realize its potential, the DPDP Act must evolve through targeted reforms, robust enforcement, and public engagement. By balancing individual rights with economic and security interests, India can build a data protection regime that empowers citizens and cements its role as a global digital leader. The path forward lies in fostering trust, innovation, and accountability in an increasingly connected world.

[1] Ministry of Electronics and Information Technology, 'India's Digital Future: A $1 Trillion Opportunity' (2024).
[2] *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[3] Information Technology Act 2000, s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[4] Justice B.N. Srikrishna Committee, 'Protecting Privacy in a Digital Economy' (2018).
[5] Digital Personal Data Protection Act 2023, s 2(t).
[6] ibid, s 2(j).
[7] ibid, s 2(i).
[8] ibid, s 6.
[9] ibid, ss 11–13.
[10] ibid, s 8.
[11] ibid, s 33.
[12] ibid, s 17.
[13] P. Sharma, 'Surveillance and Privacy in India: A Legal Analysis' (2023) 14 Journal of Privacy Studies 56.
[14] Ministry of Electronics and Information Technology, 'Draft Rules under the DPDP Act' (2025).
[15] Draft Rules 2025, s 4.
[16] Constitution of India, Eighth Schedule; Draft Rules 2025, s 6.
[17] Draft Rules 2025, s 8.
[18] DPDP Act 2023, s 10.
[19] ibid, s 27.
[20] Union Budget 2024–25, Ministry of Finance, Government of India.
[21] Regulation (EU) 2016/679 (GDPR), art 51.
[22] UK Data Protection Act 2018, s 6.
[23] Reserve Bank of India, 'ODR Framework for Digital Payments' (2024); Securities and Exchange Board of India, 'Cybersecurity Guidelines' (2024).
[24] *Puttaswamy* (n 2).
[25] *Meta Platforms Inc. v. CCI* (2024) CCI Case No. 10 of 2023.
[26] *Meta Platforms Inc. v. CCI*, NCLAT Appeal No. 1001 of 2024.
[27] *Aadhaar v. Union of India*, WP (Civil) No. 342 of 2023 (Supreme Court, pending).
[28] RBI (n 23).
[29] SEBI (n 23).
[30] Ministry of Electronics and Information Technology, 'AI Ethics Framework' (2024).
[31] GDPR, arts 15–22.
[32] ibid, art 33.
[33] DPDP Act 2023, s 17.
[34] GDPR, art 52.
[35] ibid, art 45.
[36] Singapore Personal Data Protection Act 2012.
[37] Brazil's Lei Geral de Proteção de Dados (LGPD) 2020.
[38] China's Personal Information Protection Law 2021.
[39] R. Gupta, 'Sectoral Challenges in India's Data Protection Framework' (2024) 5 Journal of Cyber Law 72.
[40] Sharma (n 13).
[41] Confederation of Indian Industry, 'Impact of DPDP Compliance on Startups' (2024).
[42] Telecom Regulatory Authority of India, 'Digital Inclusion Report 2024' (2024).
[43] A. Kumar, 'The Data Protection Board: Challenges of Implementation' (2025) 11 Indian Journal of Constitutional Law 89.
[44] S. Rao, 'Leveraging AI and Blockchain for Data Protection' (2024) 3 Journal of Data Governance 34.
[45] N. Jain, 'India as a Global Data Hub: Opportunities and Risks' (2025) 8 Journal of Digital Economy 19.
[46] *Aadhaar* (n 27).