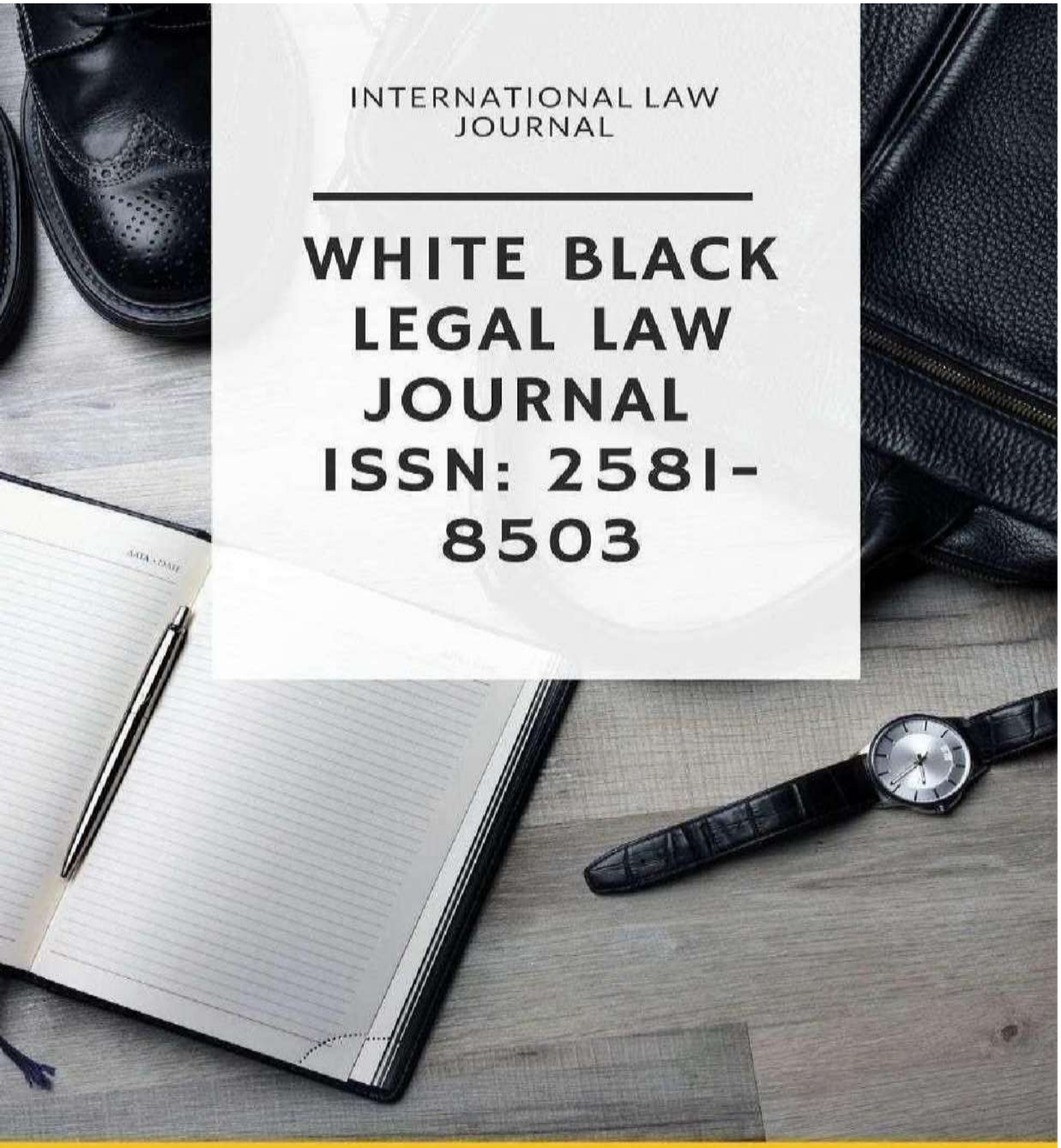

INTERNATIONAL LAW JOURNAL

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

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.

AN APPRAISAL OF INDIA'S DIGITAL PERSONAL DATA PROTECTION REGIME UNDER THE DPDP ACT, 2023

AUTHORED BY - RAKSHITA SINGH
B.A.LL.B
Trinity Institute of Professional Studies, GGSIPU, New Delhi

Abstract

An important turning point in the evolution of India's data governance framework has been reached with the passage of the Digital Personal Data Protection Act 2023. This statute is the first specific legal framework governing digital personal data in India, and it comes against the backdrop of rapidly expanding digital services, rapid digitization, and the constitutional recognition of privacy as a fundamental right. This essay examines the development of India's data protection legislation, evaluates its main features, and compares it to the EU's General Data Protection Regulation to determine whether it complies with international norms. The study argues that although the DPDP Act incorporates significant progressive features like data principal rights and consent-centric processing, structural issues with regard to enforcement independence, government exemptions, It concludes with considerations for future reform.

Introduction

Personal data is now a vital resource for governance and the economy due to the exponential growth of digital technologies. In India, massive digitization projects like Aadhaar and Digital India, as well as the growth of online platforms, have led to the processing of previously unheard-of amounts of personal data by both public and private entities. Concerns about surveillance, the abuse of personal data, and the degradation of people's information privacy have increased as a result of this change. The normative basis for statutory data protection was established by the Supreme Court's recognition of privacy as a fundamental right in Justice K S Puttaswamy (Retd) v. Union of India.[1]

[1] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

Parliament responded by passing the Digital Personal Data Protection Act 2023[2] which aims to control the processing of digital personal data using an accountability-driven and consent-based framework. In order to determine the Act's level of compliance with international data protection standards, this paper critically examines it by following the development of Indian data protection law, examining its main provisions, and conducting a comparative analysis with the General Data Protection Regulation (GDPR) of the European Union.

II. Evolution of Data Protection Law in India - A Doctrinal and Legislative Analysis

The evolution of data protection law in India is best understood as a multi-phase development encompassing judicial, policy, and legislative milestones that progressively shifted India from a rudimentary tech law regime to a dedicated statutory regime for digital personal data. These phases reflect concerns about informational privacy arising from rapid digitisation and the state's growing use of digital platforms for governance and commerce.

1. The Early Framework: The IT Act and SPDI Rules (2000–2016)

The Information Technology Act, 2000 (IT Act), which was passed to give legal recognition to digital communications and electronic transactions, was the first piece of legislation in India governing information technology. The main goals of this law were to support e-commerce and give digital signatures, cybercrimes, and record authenticity in electronic governance a legal framework.[3] Data protection as such was not a specific goal under the IT Act; rather, security procedures and protecting private data were incidental components of cyber law enforcement.

Legal Import: The early regime did not recognize privacy as an independent legal right, adopting a sector-specific regulatory approach that left significant gaps, particularly in addressing issues like consent, transparency, and enforceable personal data rights. In 2011, the government introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, [4]which were framed under the IT Act and imposed basic obligations on corporate entities

[2] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023)
[3] IT ACT 2000
[4] The Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011

collecting personal information, requiring the adoption of privacy policies, consent for data collection, and reasonable security practices.[5] On the other hand, these rules lacked comprehensive principles of purpose limitation, data subject rights, accountability mechanisms, and enforceable statutory remedies.[6]

2. Judicial Recognition of Privacy: The Puttaswamy Era (2017)

In the case of Justice K.S. Puttaswamy (Retd) v. Union of India (2017), the Supreme Court's nine-judge panel unequivocally held that the right to privacy is fundamental and inherent to Article 21 of the Indian Constitution, marking a turning point in the country's data protection jurisprudence. The Court clarified that privacy includes informational privacy, acknowledging that a person's digital information represents their autonomy, dignity, and freedom from arbitrary interference.[7]

Importantly, the Court developed a three-part test - legality, necessity, and proportionality based on international human rights standards to evaluate state interference with privacy. This constitutional standard sparked legislative and policy reactions, creating a normative framework for India's data protection legislation.

Doctrinal Significance: The Puttaswamy ruling made privacy a constitutional imperative rather than a policy debate, requiring the State to enact protective laws. It also recognized that private actors who gather and process personal data pose privacy risks just as much as the government.

3. Post-Puttaswamy Legislative Efforts: From Committee Reports to Statute (2017–2023)

A Committee of Experts led by Justice B.N. Srikrishna was established by the Union Government after Puttaswamy to discuss a comprehensive data protection framework. In its 2018 report, A Free and Fair Digital Economy: [8]Protecting Privacy, Empowering Indians, the Committee suggested a rights-based data protection law that was largely based on the GDPR and placed a strong emphasis on individual liberty, purpose restriction, data minimization, and an impartial regulatory body. These ideas were mirrored in the draft Personal Data Protection Bill, 2018 that was appended to the

[5] Evolution of Data Privacy Regime in India, 3.3 JCLJ (2023) 892
[6] Evolution of Data Privacy Regime in India, 3.3 JCLJ (2023) 892
[7] Justice K.S. Puttaswamy (Retd) v. Union of India
[8] Committee of Experts under Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) - The Hindu Centre for Politics and Public Policy

report. It called for a robust Data Protection Authority with both adjudicatory and enforcement authority.

Subsequent versions of the Bill in 2019 and 2021, however, saw these protections slowly eroded. The Personal Data Protection Bill, 2019 expanded exemptions for government and added local storage mandates. The 2021 recommendations by a Joint Parliamentary Committee [9]went further, recommending extending the law to non, personal data as well. These changes continue to be met with criticism from civil society groups, industry representatives, and academics in the country.

In 2022, the government released the Bill again, this time with a lot more reasons to oppose it, including the absence of a comprehensive legal framework[10]. The culmination of these debates, the Digital Personal Data Protection Act, 2023 (DPDP Act) adopted a wholly narrower, principles- based approach that was limited to digital personal data alone and had far fewer compliance burdens.

The DPDP Act is both 'continuity and rupture' continuity in that it recognises privacy as a protected interest and rupture in departing from the 'rights, heavy' and 'institutionally independent' model initially envisaged in the aftermath of Puttaswamy.

III. Core Features of the DPDP Act, 2023

The DPDP (Digital Personal Data Protection) Act creates a "consent centric" approach in the handling of digital personal data by "data fiduciaries". Its design is based on the following principles: a lawful basis of processing, accountability and minimal rights: the "data principals".[11]

1. Scope and Applicability

The Act governs the processing of digital personal data, which is personal data that is processed electronically within India, and extraterritorial digital processing where

[9] https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece#:~:text=Minister%20says%20he%20will%20bring,into%20the%20comprehensive%20legal%20framework.%E2%80%9D
[10] https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece#:~:text=Minister%20says%20he%20will%20bring,into%20the%20comprehensive%20legal%20framework.%E2%80%9D
[11] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section2 (j)

goods or services are provided to individuals in India. Digital processing of nonpersonal data and offline digital processing is specifically excluded from its scope, unlike the GDPR.[12] which encompasses all personal data. The Act also proposes exclusion for certain classes of data, fiduciaries, including small organizations and startups, through delegated legislation, which could lead to regulatory conflicts.

2. **Consent and Lawful Processing**

Consent under the DPDP Act must be free, specific, informed, unconditional and unambiguous through a clear, tangible affirmative act.[13] It prescribes notice requirements related to processing purpose and data principal rights. However, the Act provides sweeping anti consent grounds for "legitimate uses" such as state functions, employment purposes and law compliance. These exceptions distort consent and undermine the safeguards it offers.[14]

3. **Rights of Data Principals**

Apart from allowing access, correction, erasure, redressal and nomination rights, the Act grants rights of data portability and objection to processing, which perhaps should have been explicitly included.[15] It takes an expansive framing of rights and focuses on procedural remedies rather than individual rights.

4. **Obligations of Data Fiduciaries**

Data fiduciaries shall be required to maintain quality of data, enact appropriate security measures and to erase data after utilization ceases. Some entities may be designated as a 'significant data fiduciary', depending on volume and sensitivity of data processed, mandating higher degrees of compliance, like working out data protection impact assessment.[16] The parameters and the safeguards for approval have been left to executive discretion.

[12] https://gdpr-info.eu/art-2-gdpr/ GDPR Article 2
[13] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 6
[14] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 7
[15] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section11- 14
[16] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 8

IV. Enforcement Architecture and Government Exemptions

The DPDP Act creates the Data Protection Board of India as the primary empowered adjudicatory body to enforce the provisions of the act.[17] A seven member data protection board is established, members of which are to be appointed by the Central Government. Its independence is limited by the fact that the Board can be controlled in terms of length of term, rule, making and removal.[18] This is problematic given the Supreme Court's insistence on independent oversight as a vital component of privacy.

Further, 17 provides that the government may exempt any agency of the government from the provisions of the Act on the grounds of sovereignty, public order or national security.[19] The wide scope of this exemption, combined with the fact that there are no procedural safeguards such as a duty to be necessary and proportionate, is at loggerheads with the Puttaswamy criteria.

The concentration of exemption and enforcement powers in the executive is detrimental to the checks and balances crucial to good data protection governance.

V. Comparative Assessment with the GDPR

Comparatively, it can be seen that though the basic concept of the DPDP Act is inspired by the GDPR, the approach and substance differs to a great extent.

The GDPR espouses, not surprisingly, a universal definition of PD, across sectors, with extensive rights, competently protected by independent regulator(s)[20]. The general nature of data and weaker legislative protections under the DPDP Act, however, betrays a state, focused, compliance driven approach, evident even in the lack of binding principles of data minimisation and purpose limitation.[21]

However, the DPDP Act shares with sui generis international standards on extraterritorial reach, breach notification, and tiered sanctions. These, at least, suggest a gradual convergence between India and the rest of the world, although not to the level of the normative force of the

[17] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 18
[18] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 18 and Section 19
[19] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 Section 17(2)(a)
[20] GDPR, Article (12–22), (51–59)
[21] GDPR, art. 5 with DPDP Act, 2023

GDPR.

VI. The Road Ahead

Rather than formal enactment, the efficacy of the Digital Personal Data Protection Act, 2023 in the longer, term will ultimately hinge on the evolution of this institutional design and substantive protections in implementation and reform. Leadership in safeguarding regulatory independence is essential for the data protection landscape to remain functional and effective. Yet the Data Protection Board of India, as currently staffed, is overly reliant on the executive for power over appointments, tenure, and rules. To satisfy Puttaswamy, the Board's design would need to protect it from executive influence and allow it similar operational independence to other constitutionally mandated regulatory bodies.

Equally important is the reform of the Act's provisions to re, calibrate government exemptions. Section 17 empowers the executive with unchecked power to exempt state agencies on the grounds of sovereignty, public order and national security, without requiring checks like necessity, proportionality or periodic review. This must be set right in future revisions by legalising stringent statutory criteria with accountability standards to prevent routine and blanket exemptions, which would undermine the effectiveness of the Act and thus, the right to privacy itself.

It also continues to be critical to accelerate reforms making a broader range of substantive rights available to data principals. Without rights to data portability, to object to processing, and to powerful restrictions on automated decision, making, India's framework risks falling seriously out of step with evolving global norms, as it seeks to deepen the reach of its digital economy with private entities acting as the primary mediators of access to key services.

VI. The Road Ahead

The long-term effectiveness of the Digital Personal Data Protection Act, 2023 will depend less on its formal enactment and more on how its institutional architecture and substantive protections evolve through implementation and reform. A central priority going forward must be the strengthening of regulatory independence. The Data Protection Board of India, as presently constituted, remains heavily dependent on the executive for appointments, tenure,

and rule-making authority.[22] Aligning the Board's design with constitutional requirements articulated in Puttaswamy would require insulating it from executive control and ensuring functional autonomy comparable to independent regulatory authorities in other rights-sensitive domains.

Equally critical is the recalibration of government exemptions under the Act. Section 17 grants the executive wide discretion to exempt state agencies on grounds of sovereignty, public order, and national security, without mandating procedural safeguards such as necessity, proportionality, or periodic review.[23] Future reforms must incorporate clear statutory thresholds and oversight mechanisms to prevent routine or blanket exemptions that risk hollowing out the right to privacy. Without such constraints, the Act may legitimise precisely the forms of unchecked state surveillance that Puttaswamy sought to constitutionally restrain.

The expansion of substantive rights available to data principals also remains an urgent area for reform. The absence of rights such as data portability, the right to object to processing, and meaningful limitations on automated decision-making places India's framework at odds with emerging global standards.[24] As India's digital economy deepens and private actors increasingly mediate access to essential services, empowering individuals with greater control over their personal data will be essential to maintaining trust and democratic accountability in digital governance.

VII. Conclusion

The Digital Personal Data Protection Act, 2023 represents a significant milestone in India's constitutional and regulatory journey toward recognising privacy as a legally enforceable right. Enacted after years of deliberation following Justice K.S. Puttaswamy v. Union of India, the Act fills a longstanding legislative void by providing a statutory framework for the protection of digital personal data. It signals India's willingness to engage with global data governance norms and establishes baseline obligations for both state and private actors operating in the digital ecosystem.

[22] Digital Personal Data Protection Act, 2023, Section 19–21
[23] Digital Personal Data Protection Act, 2023, Section 17; *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1, paras 180–181
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), Article 18–21

However, the Act's transformative potential is limited by its narrow scope, diluted consent framework, constrained rights architecture, and executive-centric enforcement model. The departure from the rights-based and institutionally independent vision articulated by the Srikrishna Committee reflects a broader shift toward administrative convenience and state discretion. While the DPDP Act ensures formal compliance with the constitutional mandate to recognise privacy, it falls short of fully realising privacy as an aspect of dignity, autonomy, and individual self-determination.

Ultimately, the DPDP Act should be understood as an incremental beginning rather than a definitive settlement of India's data protection regime. Its success will be measured not merely by compliance metrics or enforcement statistics, but by its capacity to withstand constitutional scrutiny and adapt to the evolving challenges of a data-driven society. Without sustained legislative refinement and institutional strengthening, the promise of Puttaswamy risks being reduced to symbolic recognition rather than substantive protection in the digital age.