Bridging The Gap: Benchmarking India's Data Privacy Regime And Proposing A Roadmap For Alignment With Global Standards

Krishnath Shamrao Patil, Kanchankumar Tejram Shewale,
[1]IRTS Indian Railways/Student of LL.M., [2]Research Scholar,
Department of Law
[1]Rashtra Sant Tukdoji Maharaj Nagpur University, Nagpur. INDIA.
[2]Maharashtra National Law University,Nagpur, INDIA

Abstract:

In the digital age, personal data has emerged as a new form of wealth, driving the Fourth Industrial Revolution. This global data economy necessitates robust legal frameworks to protect individual privacy, a fundamental human right. This paper explores the international perspective on the right to data privacy, conducting a comparative analysis between India's evolving legal stance and established global regimes like the European Union's General Data Protection Regulation (GDPR), and laws in the United States, Canada, and Singapore.

The research establishes that while the Indian Supreme Court has unequivocally recognized the right to privacy as a fundamental right under Article 21 of the Constitution, the country lacks a dedicated, comprehensive data protection law. The analysis reveals a significant gap between this constitutional recognition and the on-ground implementation and enforcement mechanisms. In contrast, Nations with mature data protection laws have established independent regulatory authorities, clear principles for data processing, and stringent penalties for non-compliance.

The paper concludes that India stands at a critical juncture. By learning from international best practices and adapting them to its unique socio-economic context, India can enact a law that not only protects its citizens' privacy but also fosters innovation and trust in the digital economy. Specific recommendations are provided to bridge the existing legislative and implementation gaps, aiming to equip Indian society with the tools needed to navigate the complexities of data privacy in the 21st century.

Keywords: Data Privacy, Data Protection, GDPR, Digital India, Personal Data Protection Bill, Comparative Law, Fundamental Rights.

I. INTRODUCTION

The 21st century is characterized by the Datafication of human existence. Personal data, generated from online transactions, social media, healthcare, and more, has become a valuable economic asset, often termed "the new oil." While this data drives innovation and economic growth, its collection and processing without adequate safeguards pose a profound threat to individual autonomy and privacy.

The right to privacy is a complex, culturally contingent concept recognized as a fundamental human right in International instruments like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). Data protection is the legal and technical mechanism through which this right to privacy is operationalized in the information society. It involves principles like lawful processing, purpose limitation, data minimization, and accountability.

India's journey towards recognizing this right has been transformative, culminating in the landmark *Justice K.S. Puttaswamy (Retd.) vs Union of India* judgment in 2017[1], which declared the right to privacy a fundamental right. This judicial pronouncement created an urgent imperative for a dedicated data protection law. The subsequent drafting of the Personal Data Protection Bill (PDPB) signalled legislative intent, though its passage has been fraught with delays and revisions.

This paper aims to:

i. Trace the development of the right to privacy within the Indian constitutional framework.
ii. Conduct a comparative analysis of India's proposed data protection framework with key international models (EU, US, Singapore, Canada).
iii. Identify the critical gaps between India's legal position and global standards.
iv. Derive actionable recommendations to strengthen India's data protection regime for the benefit of its society and economy.

II. PRIVACY AND DATA PROTECTION UNDER THE INDIAN LEGAL SYSTEM

The Indian Constitution does not explicitly mention a "right to privacy." However, the judiciary has interpreted it as an intrinsic part of the fundamental rights to life and personal liberty (Article 21) and freedom of speech and expression (Article 19)[2].

The legal evolution began with a restrictive view in *M.P. Sharma v. Satish Chandra* (1954)[3] and *Kharak Singh v. State of U.P.* (1962)[4], where the Supreme Court was hesitant to recognize privacy as a standalone right. The tide turned with the *Puttaswamy* judgment, where a nine-judge bench unanimously held that the right to privacy is inherent to human dignity and is a fundamental right. This ruling laid the philosophical foundation for data protection, framing it as essential for individual autonomy in the digital world.

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

[2] The Constitution of India, 1950

[3] *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077

[4] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295

Responding to this, the government formed the B.N. Srikrishna Committee[5], which produced a draft Personal Data Protection Bill in 2018. The bill, and its subsequent iterations, drew heavily from the GDPR, proposing principles like:

Consent: Data processing based on free, informed, and specific consent.
Data Localization: Restrictions on transferring personal data outside India.
Individual Rights: Rights to access, correction, and the controversial "right to be forgotten."
Regulatory Body: Establishment of a Data Protection Authority (DPA) for oversight.
Penalties: Significant financial penalties for non-compliance.

However, the bill lapsed in Parliament, and a new, more streamlined Digital Personal Data Protection (DPDP) Act was finally passed in 2023. While a positive step, it has been the subject of debate regarding exemptions granted to the government and a perceived dilution of the DPA's independence[6].

III. COMPARATIVE ANALYSIS OF INTERNATIONAL DATA PROTECTION LAWS

A. The European Union's General Data Protection Regulation (GDPR)[7]

The European Union's General Data Protection Regulation (GDPR)[8] is universally regarded as the global gold standard for data protection, establishing a high-bar, rights-based framework that has influenced legislation worldwide. Its comprehensiveness is evident in its core principles, which include stringent requirements for obtaining clear and affirmative consent, granting data subjects a powerful suite of rights—such as the right to access, port, and erase their personal data—and mandating Data Protection Impact Assessments (DPIAs) for high-risk processing activities. Furthermore, its extraterritorial scope ensures that any entity processing the data of EU citizens, regardless of its physical location, must comply, a feature that has given the regulation immense global reach. The potency of the GDPR is underscored by its enforcement mechanism, which can levy devastating fines of up to 4% of a company's annual global turnover. This model heavily inspired India's initial 2018 Personal Data Protection Bill (PDPB). However, a critical divergence emerges in the final Digital Personal Data Protection (DPDP) Act of 2023, particularly regarding the balance of power. Unlike the fiercely independent data protection authorities (DPAs) in the EU that enforce the GDPR without political interference, India's Act grants significant exemptions to government agencies and empowers the central government to override the rulings of the Data Protection Board of India in certain cases. This creates a substantial distinction in oversight and implementation, positioning the Indian framework as more state-centric compared to the individual-centric, autonomously enforced model of the GDPR.

[5] Government of India. (2018). Report of the Expert Committee on a Data Protection Framework for India (Chairperson: Justice B.N. Srikrishna)
[6] Government of India. The Digital Personal Data Protection Act, 2023

[7] European Union. (2016). General Data Protection Regulation (GDPR)
[8] European Union. (2016). General Data Protection Regulation (GDPR)

B. The United States: A Sectoral Approach

In stark contrast to the comprehensive, horizontal approach of the EU's GDPR, the United States employs a fragmented, sector-specific model for data privacy, lacking an overarching federal law. This patchwork system targets specific industries and vulnerabilities through legislation like the Children's Online Privacy Protection Act (COPPA)[9], which safeguards the personal information of children under 13, and the Health Insurance Portability and Accountability Act (HIPAA), which creates strict standards for protecting sensitive patient health data. Furthermore, due to congressional gridlock on federal privacy law, state-level initiatives have filled the void, most notably California's legislation[10]. The California Online Privacy Protection Act (CalOPPA) and its significantly stronger successor, the California Privacy Rights Act (CPRA), have effectively set de facto National standards by compelling companies that operate nationwide to extend these Californian rights to a vast majority of American consumers. This comparison highlights a fundamental philosophical divergence in legislative strategy[11]. where the U.S. has opted for targeted, reactive measures, India is consciously pursuing a unified, horizontal framework akin to the GDPR with its Digital Personal Data Protection Act. This choice promises more uniform and consistent protection for all citizens across all sectors of the economy. However, this comprehensive model's success is entirely contingent upon the establishment of a powerful, truly independent, and well-resourced Data Protection Authority (DPA) capable of effective enforcement against both private entities and government bodies—a formidable institutional challenge that India must now overcome.

C. Canada's PIPEDA

Canada's approach to data privacy is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA), a comprehensive federal law that applies to the private sector. Unlike a rigid, prescriptive set of rules, PIPEDA is fundamentally principle-based, built upon ten fair information principles. Its core tenet is the requirement for knowledge and consent, mandating that organizations must obtain an individual's understanding and permission for the collection, use, or disclosure of their personal information. This makes it structurally similar to India's chosen path with the Digital Personal Data Protection (DPDP) Act, as both represent a unified, horizontal framework rather than a sectoral patchwork. A critical lesson for India from the Canadian model lies in the role and function of its oversight body. PIPEDA is enforced by the Office of the Privacy Commissioner of Canada (OPC), an independent ombudsman vested with significant powers to investigate public complaints, conduct audits, and promote compliance through guidance and recommendations. While the OPC's decisions are not always directly binding and can be appealed to federal courts, its authority as a proactive, investigative, and highly visible public advocate for privacy rights has been instrumental in building a culture of compliance[12]. For India's nascent Data Protection Board (DPB), emulating this model—functioning not merely as a passive adjudicator but as an active, independent guardian of citizen rights—

[9] United States. Children's Online Privacy Protection Act (COPPA), 1998
[10] United States. Health Insurance Portability and Accountability Act (HIPAA), 1996
[11] California Online Privacy Protection Act (CalOPPA), 2004
[12] Canada. Personal Information Protection and Electronic Documents Act (PIPEDA), 2000

could be pivotal in ensuring the DPDP Act's principles are effectively translated into meaningful practice.

D. Singapore's PDPA

Singapore's Personal Data Protection Act (PDPA) exemplifies a pragmatic, hybrid approach to data governance, deliberately engineered to strike a careful balance between safeguarding individual privacy and facilitating economic growth and innovation. It is consciously less stringent than the GDPR, employing more flexible concepts like "deemed consent" in certain business contexts and offering broader exemptions for legitimate business practices. This design makes it highly effective within Singapore's specific context as a global business hub with a relatively small, digitally literate population. The comparison with India, however, reveals a critical divergence in necessary priorities. While Singapore's business-centric model offers a valuable lesson in crafting legislation that is commercially pragmatic without being weak, India's context is fundamentally different. Its vast population of over 1.4 billion people, coupled with a significant digital divide and varying levels of digital literacy, creates a landscape where individuals are often more vulnerable to exploitation. Therefore, India's Digital Personal Data Protection Act cannot afford to lean as heavily towards business facilitation. Instead, it necessitates a stronger, more individual-centric protective framework—akin to the GDPR—that proactively empowers citizens, imposes stricter obligations on data fiduciaries, and ensures robust oversight to safeguard the rights of a billion-plus citizens who are at the heart of its digital transformation[13].

IV. CRITICAL GAPS AND ANALYSIS

The comparative study reveals several gaps in the Indian approach:

1. **Implementation Gap:** The foremost challenge is moving from a law on paper to effective enforcement. The independence, capacity, and resources of the proposed Data Protection Board of India will be the true test.
2. **Government Exemptions:** The wide exemptions granted to government agencies in the DPDP Act for reasons of National security and public order create a significant loophole, potentially leaving a vast amount of citizen data without adequate protection against state surveillance.
3. **Dilution of Provisions:** The journey from the 2018 draft bill to the 2023 Act saw the removal of several progressive features, such as penalties for violating the right to privacy itself (not just the law) and a weaker framework for processing non-personal data.

[13] Singapore. Personal Data Protection Act (PDPA), 2012.

4. **Adequacy Challenges:** For India to become a global data hub, the European Commission must grant it an "adequacy decision," confirming that its data protection standards are equivalent to the GDPR's. The current exemptions and perceived lack of DPA independence could be a significant hurdle in securing this status, impacting international business.

V. RECOMMENDATIONS FOR THE INDIAN SOCIETY

Based on the international comparative analysis, the following recommendations are proposed to ensure the data protection regime benefits Indian society:

A. **Ensure Regulatory Independence:** The Data Protection Board must be constituted as a fully autonomous body, insulated from political interference, with its members having security of tenure. Its decisions should be subject only to judicial review.

B. **Promote Digital Literacy:** The government should launch massive public awareness campaigns to educate citizens about their data rights, how to give informed consent, and the mechanisms for reporting violations. A law is only powerful if people know how to use it.

C. **Review Government Exemptions:** The exemptions for government processing should be narrowed and subjected to a system of independent oversight, perhaps requiring judicial warrant or approval from the DPA for certain types of data access, ensuring a check on state power.

D. **Incentivize Privacy by Design:** Encourage and incentivize businesses to embed privacy-enhancing technologies (PETs) and data protection measures into the design of their products and services from the outset, not as an afterthought.

E. **Strengthen Penalties and Grievance Redressal:** The penalty structure should be robust enough to act as a deterrent for large corporations. Furthermore, the process for individuals to file complaints must be simple, accessible, and inexpensive.

VI. CURRENT STATUS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, though enacted after receiving Presidential assent and publication in the Gazette on 11 August 2023, has not yet come into force as no effective date has been notified by the Central Government.[14] To operationalize the law, the Ministry of Electronics and Information Technology (MeitY) issued the *Digital Personal Data Protection Rules, 2025* on 3 January 2025 for public consultation, with feedback invited until 5 March 2025.[15] By 26 July 2025, the government had received 6,915 responses from citizens and stakeholders, reflecting wide public and institutional engagement with the proposed regulatory framework.[16] Despite this progress, as

[14] *Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Gazette of India, Aug. 11, 2023

[15] Press Release, Ministry of Electronics & Info. Tech., Govt. of India, *Draft Digital Personal Data Protection Rules, 2025 Released for Public Consultation* (Jan. 3, 2025), available at https://pib.gov.in/PressReleasePage.aspx?PRID=2148944.

[16] Id. (noting that 6,915 responses were received by July 26, 2025)

of August 2025, the Act remains unenforced because the final rules have not been officially notified and the Data Protection Board of India (DPBI), the adjudicatory body for handling complaints, breaches, and penalties, is yet to be constituted.[17] The next steps anticipated include notifying the final rules, appointing staggered commencement dates for different provisions of the Act, and formally establishing the DPBI.[18] Until then, India continues to rely on the existing framework under the Information Technology Act, 2000 and related rules. For businesses and government agencies, this means there is currently no binding enforcement of the DPDP Act, but proactive compliance preparations are strongly advisable, particularly concerning consent, notice requirements, data security measures, and breach reporting protocols. Implementation is expected in a phased manner once the rules are finalized and institutional mechanisms are in place, making readiness a key priority for all stakeholders.

VII. CONCLUSION

The DPDP Act represents a significant milestone in India's journey toward a robust data protection regime, aligning national standards with global privacy norms. However, its delayed enforcement highlights the challenges of building comprehensive institutional mechanisms, ensuring stakeholder consensus, and balancing regulatory oversight with ease of doing business. While the Act's implementation is imminent, its success will depend on timely notification of the rules, effective functioning of the Data Protection Board of India, and phased compliance strategies that provide clarity and predictability for organizations and citizens alike. As the comparative analysis with international frameworks shows, the true measure of success will lie in effective implementation. The gaps in enforcement, oversight, and balancing state power with individual rights need to be addressed with urgency and foresight. By learning from the successes and failures of mature regimes like the GDPR and adapting them to India's unique democratic fabric and developmental context, India can forge a path that truly protects its billion-plus citizens. A robust, fair, and trusted data protection ecosystem is not a barrier to innovation and governance; it is its very foundation. It will empower Indian citizens, build trust in the digital economy, and position India as a responsible leader in the global digital order. The promise of a Digital India can only be fully realized when every citizen is confident that their digital self is protected by the rule of law.

[17] India's Long Wait for Data Protection Law, *Econ. Times* (Aug. 2025), https://economictimes.indiatimes.com/tech/technology/indias-long-wait-for-data-protection-law/articleshow/123223043.cms

[18] Hogan Lovells, *India Publishes Consent Management Rules Under DPDP Act* (Aug. 2025), https://www.hoganlovells.com/en/publications/india-publishes-consent-management-rules-under-digital-personal-data-protection-act

VIII. REFERENCES

[1] The Constitution of India, 1950.

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

[3] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

[4] *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077.

[5] European Union. (2016). General Data Protection Regulation (GDPR).

[6] Government of India. (2018). Report of the Expert Committee on a Data Protection Framework for India (Chairperson: Justice B.N. Srikrishna).

[7] Government of India. The Digital Personal Data Protection Act, 2023.

[8] United States. Children's Online Privacy Protection Act (COPPA), 1998.

[9] United States. Health Insurance Portability and Accountability Act (HIPAA), 1996.

10] California Online Privacy Protection Act (CalOPPA), 2004.

[11]Canada. Personal Information Protection and Electronic Documents Act (PIPEDA), 2000.

[12] Singapore. Personal Data Protection Act (PDPA), 2012.