THE LEGAL FRAMEWORK OF DATA PROTECTION IN INDIA: THE NEED FOR A COMPREHENSIVE DATA PROTECTION LAW

Tansi Mehrotra[1], IILM University, Gurugram

ABSTRACT

In the age of rapid technological advancements and increasing digitalisation, the collection, processing, and transfer of personal data is integral to economic and social life. India, as one of the largest digital economies, faces unique challenges in balancing technological growth with the protection of individual privacy. Despite the recognition of privacy as a fundamental right by the Supreme Court in 2017, India's legal regime for data protection remains fragmented and inadequate. This paper critically examines the existing legal and regulatory framework governing data protection in India, analyses its gaps, explores global best practices, and argues for the urgent need for a sturdy, comprehensive, rights-centric data protection law to ensure accountability, transparency, and trust in the digital ecosystem.

Keywords: Data Protection; Data Privacy; Digital Personal Data Protection Act, 2023; Personal Data Protection Bill, 2019; Right to Privacy; Justice K.S. Puttaswamy (Retd.) v. Union of India; Information Technology Act, 2000; GDPR; California Consumer Privacy Act (CCPA); Brazil's Lei Geral de Proteção de Dados (LGPD); Consent-based Processing; Data Fiduciaries; Data Principals; Cross-border Data Transfers; Governmental Exemptions; Data Protection Board of India; Privacy by Design; Fundamental Rights; Informational Privacy; Surveillance; Institutional Independence; Digital Governance; Comparative Data Protection; Constitutional Morality.

[1] 2nd Year Law Student, BBA LLB (H.)

1.Introduction

India stands at the forefront of a digital revolution. With over a billion citizens increasingly connected through Aadhaar-linked services, Unified Payments Interface (UPI), e-commerce platforms, fintech innovations, and social media networks, the country has witnessed an unprecedented surge in data generation and exchange. This rapid digitisation has transformed the Indian economy, enabling financial inclusion, streamlining governance, and fostering entrepreneurial growth. However, it has also brought to light a new era of vulnerability where personal data, often described as the "new oil"[2] of the 21st century, is extracted, processed, and monetised with limited oversight. Beyond its economic value, data is intrinsically tied to individual autonomy, dignity, and freedom, making its protection not just a commercial imperative but a fundamental rights issue.[3]

Despite the centrality of data in India's digital ecosystem, the legal framework governing its protection remains fragmented and outdated. Historically, the Information Technology Act, 2000 (IT Act), along with sector-specific regulations and the 2011 Privacy Rules, formed the backbone of India's data protection regime. These instruments, however, were never designed to address the complexities of modern data ecosystems.[4] They offer limited safeguards, lack robust enforcement mechanisms, and fail to provide comprehensive rights to data subjects. The IT Act, for instance, focuses more on cybersecurity and electronic commerce than on personal data protection, leaving significant gaps in areas such as consent, data minimisation, purpose limitation, and cross-border data transfers.

The inadequacy of India's existing legal framework became starkly evident in the wake of the Supreme Court's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[5], which unequivocally recognised the right to privacy as a fundamental right under Article 21 of the Constitution. This constitutional affirmation catalysed a nationwide demand for a dedicated data protection law that would align with global standards and safeguard citizens against misuse, surveillance, and exploitation of their personal information. In

[2]Nisha Talagala, "Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires" *Forbes*, 2022*available at*: https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/.
[3] Manupatra, "Articles – Manupatra" *Manupatra.com*, 2025*available at*: https://articles.manupatra.com/article-details/From-Constitutional-Rights-to-Data-Protection-Article-21-and-Comparative-Perspectives-on-Privacy.
[4] "Corpzo," *Digital India Act,2025: A Much-Needed Update to the IT Act,2000* , 2025*available at*: https://www.corpzo.com/digital-india-act-2025-a-muchneeded-update-to-the-it-act-2000.
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

response, the Indian government initiated a series of consultations and legislative drafts, culminating in the enactment of the Digital Personal Data Protection Act (DPDP Act), 2023.

The DPDP Act[6] marks India's first attempt at a comprehensive data protection legislation. It introduces key principles such as lawful processing, consent-based data collection, rights of data principals, and obligations for data fiduciaries. It also establishes a Data Protection Board to oversee compliance and adjudicate disputes. However, the Act has drawn mixed reactions from legal scholars, civil society, and industry stakeholders. While it represents a significant step forward, critics argue that it falls short in several areas—such as the scope of exemptions granted to the government, the absence of strong accountability mechanisms, and limited transparency in enforcement. Moreover, the Act's applicability is restricted to digital personal data, leaving non-digital and non-personal data outside its ambit.

In contrast, the European Union's General Data Protection Regulation (GDPR)[7], widely regarded as the gold standard in data protection, offers a more powerful and rights-centric approach. The GDPR enshrines principles of transparency, accountability, and user empowerment, with stringent penalties for non-compliance. It provides individuals with a suite of rights—including the right to access, rectify, erase, and port their data—and mandates data protection by design and default. The regulation also imposes strict conditions on cross-border data transfers and requires organisations to appoint Data Protection Officers under certain circumstances. India's DPDP Act, while inspired by the GDPR, diverges significantly in its treatment of state surveillance, enforcement independence, and user rights.[8]

This research paper seeks to critically examine the current legal framework for data protection in India, with a focus on the DPDP Act and its limitations. It aims to answer four key questions: (1) Does India's existing legal regime adequately safeguard personal data? (2) What are its major gaps and challenges? (3) What lessons can be drawn from comparative jurisdictions such as the EU's GDPR? (4) What should a truly comprehensive data protection law in India contain to ensure both economic innovation and constitutional fidelity?

By exploring these questions, the paper hopes to contribute to the ongoing discourse on data governance in India and advocate for a legal architecture that balances technological progress

[6] Digital Personal Data Protection Act, 2023
[7] EU General Data Protection Regulation (GDPR), 2016
[8] Latham&Watkins LLP, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison*, 2023.

with individual rights. In an age where data is power, the need for a secure, transparent, and rights-respecting data protection law is not just desirable, it is indispensable.

2.Concept of Data Protection

Data protection refers to the legal measures taken to safeguard personal information from misuse, unauthorized access, or disclosure. Personal data may include names, addresses, contact numbers, financial information, biometric data, and other sensitive details that can identify an individual. The Digital Personal Data Protection Act (DPDP), 2023, defines personal data as any data about an individual who is identifiable by or in relation to such data.[9]

At its core, data protection encompasses principles such as informed consent, purpose limitation, data minimization, accountability, and transparency. These principles guide how data should be collected, processed, stored, and shared. The concept also includes the rights of individuals such as the right to access, correct, and delete their data and the obligations of data controllers and processors to implement security measures and respond to breaches. It ensures that individuals retain autonomy over their personal information and that organizations handle such data responsibly.[10]

As digital technologies permeate every aspect of life the volume and sensitivity of personal data being collected, processed, and stored has also grown exponentially. This has heightened the need for strong data protection frameworks that balance individual privacy rights with the legitimate interests of businesses and governments. With the increasing reliance on digital services, protecting such data is essential to uphold individual privacy, ensure national security, and build public trust in digital governance.

3.Evolution of Data Protection Law in India

3.1 Early Legislative Measures

India's first attempt to regulate the digital space came with the enactment of the **Information Technology Act, 2000 (IT Act, 2000)**. The primary objective of this legislation was to

[9] Digital Personal Data Protection Act, 2023

[10] "What is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know," *www.digitalguardian.comavailable at*: https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you.

facilitate the growth of electronic commerce by granting legal recognition to electronic transactions, digital records, and electronic signatures, thereby encouraging trust in digital platforms. Data protection, however, was not the central focus of the statute and found only limited recognition through certain provisions. **Section 43A** imposed liability on body corporates that failed to implement "reasonable security practices and procedures" resulting in wrongful loss or gain to any person, thereby introducing a basic standard of accountability for data handlers. Complementing this, **Section 72A** criminalised the disclosure of personal information without consent, when such disclosure occurred in the course of lawful contracts.[11]

Judicial interpretation of these provisions highlighted both their utility and their inadequacies. In *ICICI Bank Ltd. v. Shanti Devi Sharma*[12], the Court dealt with the unauthorised disclosure of a borrower's personal details by recovery agents engaged by the bank. The Court held that such mishandling of sensitive customer data could give rise to liability under Section 43A, signalling the judiciary's willingness to extend statutory protections to instances of corporate negligence in data handling. A more significant challenge to the framework emerged in *Karmanya Singh Sareen v. Union of India*[13], where petitioners argued that WhatsApp's decision to share user data with Facebook violated the right to privacy and lacked adequate safeguards under the IT Act and the 2011 Sensitive Personal Data or Information Rules (SPDI Rules). Although the Court allowed users to opt out, it acknowledged that the absence of a dedicated data protection statute made it difficult to balance corporate practices with the protection of individual rights.

These cases reveal that Sections 43A and 72A were invoked only in limited factual contexts, tied either to contractual breaches or narrow consumer protection concerns, and were insufficient to address the complexities of modern digital ecosystems. The absence of clear definitions of personal and sensitive data, coupled with weak enforcement, rendered the IT Act inadequate in safeguarding informational privacy. Thus, while progressive for its time, the IT Act was ultimately ill-suited to meet the challenges of large-scale data processing, paving the way for demands for a comprehensive data protection framework.

[11] Information Technology Act, 2000
[12] Amit Ghodke, "ICICI Bank vs. Shanti Devi Sharma & Others" *Unfoldlaw*, 2024*available at*: https://unfoldlaw.in/icici-bank-vs-shanti-devi-sharma-others/.
[13] Manupatra, Karmanya Singh and Sareen Vs, *Constitutional Bench Update WhatsApp Privacy Policy*.

3.2 Puttaswamy Judgment: A Constitutional Paradigm Shift

The Supreme Court's decision in **Justice K.S. Puttaswamy (Retd.) v. Union of India** marked a decisive turning point in India's constitutional and data protection landscape. A nine-judge bench unanimously held that the **right to privacy is a fundamental right** guaranteed under Articles 14, 19, and 21 of the Constitution. The case stemmed from challenges to the Aadhaar programme, which required citizens to submit biometric and demographic data for access to welfare benefits, raising concerns of excessive state surveillance and the absence of adequate safeguards. In resolving the matter, the Court expressly overruled earlier precedents such as *M.P. Sharma v. Satish Chandra*[14] (1954) and *Kharak Singh v. State of Uttar Pradesh*[15] (1962), which had previously denied privacy the status of a constitutional right.

The judgment framed privacy as an essential attribute of dignity, liberty, and personal autonomy, thereby embedding it within the core of constitutional democracy. Crucially, it recognised **informational privacy** the protection of personal data against misuse as a distinct and pressing concern in the digital age. The Court observed that the State's role was not limited to refraining from unjustified intrusions but extended to creating a legal and regulatory framework that actively safeguards individual privacy. This recognition underscored the need for statutory data protection measures capable of addressing the risks posed by large-scale data collection, profiling, and commercial exploitation of personal information.

By constitutionalising privacy, the Puttaswamy ruling provided the **jurisprudential foundation** for India's data protection regime. It transformed privacy from a peripheral notion into a binding constitutional guarantee and placed a clear obligation on the legislature to enact comprehensive data protection legislation. The judgment not only catalysed the drafting of the Personal Data Protection Bill, 2019 but also laid the normative groundwork for the eventual passage of **t**he **Digital Personal Data Protection Act, 2023**, representing a shift from fragmented protections under the IT Act to a rights-based approach to informational privacy.

3.3 Personal Data Protection Bill, 2019

The **Personal Data Protection Bill, 2019 (PDP Bill)** represented India's first comprehensive legislative effort to establish a rights-based framework for the protection of personal data.

[14] M.P. Sharma Vs Satish Chandra 1954 AIR 300 SCR 1077
[15] Kharak Singh Vs State of Uttar Pradesh 1962 AIR 1295 SCR (1) 332

Drafted by the **Justice B.N. Srikrishna Committee**[16], the Bill was introduced in Parliament in December 2019 in direct response to the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). It sought to create a legal architecture comparable to the European Union's **General Data Protection Regulation (GDPR),** balancing individual privacy with legitimate state and business interests in data processing.

The PDP Bill defined key terms such as "personal data," "sensitive personal data," and "critical personal data," and established a detailed framework governing the collection, storage, and processing of such information. It introduced the concept of **data fiduciaries** and **data principals,** mirroring the controller-data subject relationship under the GDPR. The Bill required data fiduciaries to process data only for clear, lawful, and specific purposes and to obtain the **free, informed, and explicit consent** of the data principal prior to processing. It also recognised individual rights to confirmation and access, correction, data portability, and the right to be forgotten.[17]

One of the most significant institutional features proposed by the Bill was the creation of an independent **Data Protection Authority (DPA)** to oversee compliance, investigate breaches, and impose penalties. However, the Bill also faced criticism for providing **broad government exemptions** under Clauses 35 and 36[18], which allowed the State to process personal data without consent on grounds such as national security, public order, and sovereignty. Created a blanket exemption for the State urging critics to argue that these provisions diluted the essence of informational privacy as articulated in Puttaswamy, potentially legitimising mass surveillance. Additionally, the Bill's provisions on **data localisation**, mandating storage of certain categories of data within India, raised concerns about trade barriers and operational burdens for multinational corporations.

Despite these criticisms, the PDP Bill, 2019 marked a transformative moment in India's data protection discourse. It established the conceptual and regulatory foundation for modern data governance and initiated a nationwide debate on the balance between privacy, innovation, and security.[19] Though the Bill was ultimately withdrawn in 2022 following extensive stakeholder

[16] B.N. Srikrishna Committee Report (2018)
[17] D Shashi Tharoor, *THE DATA PRIVACY and PROTECTION BILL, 2019*.
[18] The Personal Data Protection Bill, 2019
[19] Salman Waris, "Personal Data Protection Bill 2019: an ambiguous initiative or a compliance nightmare" *Ibanet.org*, 2019*available at*: https://www.ibanet.org/article/5E76F6A3-8304-43DE-86AF-0A56F9862CE3

consultation and criticism, it directly led to the drafting of the **Digital Personal Data Protection Act, 2023,** which streamlined many of its provisions while retaining its core objective of safeguarding personal data within a rapidly digitising society.

3.4 Digital Personal Data Protection Act, 2023

The enactment of the **Digital Personal Data Protection Act, 2023 (DPDP Act)** marks a defining moment in India's data protection journey. Passed by Parliament in August 2023, the Act establishes the country's first dedicated statutory framework for the governance of digital personal data, replacing the fragmented provisions of the Information Technology Act, 2000. It embodies the legislative fulfilment of the constitutional mandate set forth in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which recognised privacy as a fundamental right. Unlike its predecessor, the Personal Data Protection Bill, 2019, the DPDP Act adopts a more **simplified, technology-neutral, and consent-centric model,** designed to balance individual rights with innovation and economic growth in a rapidly digitalising ecosystem.

The DPDP Act applies exclusively to **digital personal data**, whether collected online or digitised from offline sources, processed within India or outside if related to Indian data principals. It identifies two key actors: the **Data Fiduciary**, who determines the purpose and means of processing, and the **Data Principal**, the individual to whom the data relates.[20] The Act introduces a structured framework of rights for Data Principals, including the **right to access, right to correction and erasure,** and the **right to grievance redressal**. Consent remains the primary basis for lawful processing, which must be free, informed, specific, and unambiguous. However, the Act also recognises certain **legitimate uses** where consent is not required, such as for state functions, legal obligations, or emergencies, thereby reflecting a pragmatic approach to data processing.[21]

A significant institutional innovation of the Act is the establishment of the **Data Protection Board of India (DPBI)**, empowered to inquire into breaches, impose penalties, and ensure compliance. Penalties under the Act are substantial, extending up to ₹250 crore[22] for serious

[20] Shreya Suri, "DPDP and the criticality of data: A turning point for India's digital future" *Times of India Voices* (Times of India, 2025)*available at*: https://timesofindia.indiatimes.com/blogs/voices/dpdp-and-the-criticality-of-data-a-turning-point-for-indias-gigital-future/

[21] EY, "Decoding the Digital Personal Data Protection Act, 2023" *Ey.com*, 2023*available at*: https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023.

[22] "Enforcement and Penalties under the DPDPA, 2023 and Draft DPDP Rules, 2025," *Tsaaro*, 2025*available at*: https://tsaaro.com/blogs/enforcement-and-penalties-under-the-dpdpa-2023-and-draft-dpdp-rules-2025/

contraventions, signalling a shift towards stronger enforcement. The Act also emphasises **obligations of Data Fiduciaries**, including implementation of reasonable security safeguards, prompt breach reporting, and adherence to data minimisation and purpose limitation principles. Moreover, it allows for **categorisation of "Significant Data Fiduciaries"**[23]**,** such as large-scale processors, who are subject to enhanced compliance requirements, including data protection impact assessments and appointment of data protection officers.

However, the DPDP Act has also attracted criticism for its **broad governmental exemptions** under Section 17[24], which permit the Central Government to exempt any instrumentality of the State from compliance on grounds such as sovereignty, public order, or security of the State. Scholars argue that such unqualified powers risk undermining the privacy guarantees affirmed in *Puttaswamy* and could enable disproportionate surveillance. Furthermore, the **absence of certain rights** such as data portability and the right to object to processing places the Indian framework at variance with international standards like the EU's GDPR.[25] The **Data Protection Board's limited independence**, given that its members are appointed by the Central Government, further raises concerns regarding institutional autonomy.

The **Digital Personal Data Protection Act, 2023** represents a long-awaited and ambitious attempt to modernise India's digital data protection framework in harmony with constitutional principles and global best practices. It provides a structured, rights-based regime emphasising transparency, consent, and accountability, the pillars that were absent from earlier legal instruments. However, the Act's efficacy will depend heavily on the **independence of enforcement bodies**, the **precision of its subordinate rules**, and the **judicial interpretation** of its broad exemption clauses.

Ultimately, while the DPDP Act is not without flaws, it signifies a **foundational shift** in India's approach to data governance from fragmented regulation to a unified legal framework that recognises privacy as a core democratic value. If implemented with integrity, proportionality, and respect for fundamental rights, it could serve as a robust blueprint for balancing **individual**

[23] "Significant Data Fiduciary under DPDA 2023," *Dpo-india.com*, 2023*available at*: https://dpo-india.com/Blogs/significant-data/
[24] Digital Personal Data Protection Act, 2023
[25] Ben Dooley, " Back to Blogs Navigating Data Privacy Regulations: Comparative Insights into GDPR, CCPA, LGPD, PDPA, and Privacy Act" *Infocepts Data & AI*, 2023*available at*: https://www.infocepts.ai/blog/navigating-data-privacy-regulations-comparative-insights-into-gdpr-ccpa-lgpd-pdpa-and-privacy-act/.

privacy, state interest, and digital innovation in the decades to come.

4.Comparative Analysis: GDPR – California Consumer Privacy Act (CCPA) – Brazil's LGPD vs. India's Data Protection Regime

4.1 Introduction

The global evolution of data protection law reflects a growing recognition of informational privacy as an essential component of individual autonomy and democratic governance. The European Union's **General Data Protection Regulation (GDPR)**, the **California Consumer Privacy Act (CCPA)** in the United States, and Brazil's **Lei Geral de Proteção de Dados (LGPD)** collectively set high benchmarks for data protection standards worldwide. Each regime, while sharing common principles such as consent, transparency, and accountability, embodies distinct cultural, legal, and policy perspectives.

India's **Digital Personal Data Protection Act, 2023 (DPDP Act)** emerges as a late entrant in this global landscape, influenced by the GDPR's architecture yet tailored to domestic priorities of **digital inclusion, innovation, and state sovereignty**. A comparative analysis of these frameworks is crucial to evaluate India's readiness to meet international standards and identify potential areas for reform.

4.2 The European Union's General Data Protection Regulation (GDPR)

The GDPR, implemented in 2018[26], stands as the gold standard for data protection worldwide. It establishes a comprehensive, rights-based, and principle-driven framework governing the processing of personal data within the European Union. Central to the GDPR are its foundational principles—lawfulness, fairness, transparency, purpose limitation, and accountability—which ensure that individuals retain control over their personal information.

The GDPR requires explicit, informed consent for most forms of data processing and grants individuals a wide array of rights, including the right to access, rectification, erasure (right to be forgotten), data portability, and the right to object to automated decision-making. It imposes strict obligations on Data Controllers and Processors, mandating Data Protection Impact Assessments (DPIAs), maintenance of processing records, and breach notification within

[26] EU General Data Protection Regulation (GDPR), 2016

seventy-two hours. Enforcement is carried out by independent supervisory authorities in each member state, coordinated through the European Data Protection Board (EDPB), ensuring harmonisation across the Union.[27]

Significantly, the GDPR's penalties are stringent, extending up to €20 million or 4% of a company's global annual turnover, whichever is higher. This robust enforcement mechanism underscores the European Union's recognition of data protection as a fundamental human right under the Charter of Fundamental Rights of the European Union, embedding privacy at the heart of democratic governance and digital trust.

4.3 The California Consumer Privacy Act (CCPA), 2018

The **California Consumer Privacy Act (CCPA),** which came into force in 2020[28], marks the United States' first major attempt at a comprehensive data privacy law. Unlike the GDPR, which adopts a human rights-based approach, the CCPA is grounded in **consumer protection principles**, reflecting the U.S. emphasis on market regulation and limited federal intervention.[29]

The CCPA grants California residents the **right to know** what personal data businesses collect, the **right to delete** such data, and the **right to opt-out** of its sale. Businesses are required to disclose data collection practices and respond to consumer requests within statutory timelines. The law applies to for-profit entities that meet certain thresholds, such as annual gross revenue exceeding $25 million or handling the data of 50,000 or more consumers annually.[30]

Enforcement authority rests with the **California Privacy Protection Agency (CPPA)** and the **California Attorney General**, marking a significant shift in the American privacy landscape, which has traditionally relied on **sector-specific regulations** such as HIPAA, **Health Insurance Portability and Accountability Act**, a U.S. federal law enacted in **1996** to protect sensitive patient health information and GLBA **Gramm-Leach-Bliley Act (GLBA)**, also

[27] Vaibhav Yadav, "Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US," 1 *Journal on Development of Intellectual Property and Research* 38–51 (2025).
[28] The California Consumer Privacy Act, 2018
[29] Ruby Jug, Kevin Kalia and Muhammad Muhammad Suleiman, "Comparative Analysis of Global Privacy Laws: CCPA, GDPR, and Emerging Data Protection Frameworks Ruby Jug" *ResearchGate* (unknown, 2021)*available at :* https://www.researchgate.net/publication/395917600_Comparative_Analysis_of_Global_Privacy_Laws_CCPA_GDPR_and_Emerging_Data_Protection_Frameworks_Ruby_Jug
[30] "California Consumer Privacy Act (CCPA) Fines and Consumer Damages - Clarip," *Clarip.com*, 2020*available at*: https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/.

known as the **Financial Services Modernization Act of 1999**, is a U.S. federal law that governs how financial institutions handle consumers' personal financial information.[31]

While less comprehensive than the GDPR, the CCPA represents a **consumer empowerment model**, emphasising transparency and corporate accountability rather than fundamental rights protection.

4.4 Brazil's Lei Geral de Proteção de Dados (LGPD), 2018

Brazil's **Lei Geral de Proteção de Dados (LGPD)**, enacted in 2018 and implemented from 2020, is often regarded as Latin America's response to the GDPR. The LGPD establishes a **hybrid model** that integrates the GDPR's rights-oriented framework with Brazil's developmental priorities. It applies to all data processing operations conducted in Brazil or targeting individuals within its jurisdiction, regardless of where the processor is located.[32]

The LGPD recognises **ten legal bases** for data processing, including consent, contractual necessity, compliance with legal obligations, and legitimate interest. It grants individuals the right to access, correct, delete, and port their personal data. The law mandates that organisations appoint **Data Protection Officers (DPOs)** and conduct **impact assessments** where processing poses significant risks.[33]

To oversee enforcement, Brazil established the **National Data Protection Authority (ANPD)**, which functions as a semi-autonomous regulatory body. The LGPD prescribes penalties of up to **2% of the company's revenue**, capped at 50 million Brazilian reais per violation.[34] The Brazilian model's strength lies in its **balanced approach**, combining strong rights protections with an appreciation for the needs of a developing digital economy.

4.5 India's Data Protection Regime

India's **Digital Personal Data Protection Act, 2023 (DPDP Act)**, while influenced by the

[31] State of California Department of Justice, "California Consumer Privacy Act (CCPA)" *State of California - Department of Justice - Office of the Attorney General*, 2024*available at*: https://oag.ca.gov/privacy/ccpa.
[32] OneTrust, "LGPD vs. GDPR" *OneTrustavailable at*: https://www.onetrust.com/blog/lgpd-vs-gdpr/.
[33] Usercentrics, "LGPD: An overview of Brazil's General Data Protection Law" *Consent Management Platform (CMP) Usercentrics*, 2022*available at*: https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-law-overview/.
[34] João Bruno Soares, "Fines in LGPD - What are they, amounts, and compliance deadlines" *Plataforma de Adequação a LGPD – AdOpt available at*: https://goadopt.io/en/blog/fines-in-LGPD/.

GDPR, takes a markedly different approach that reflects India's socio-political and administrative realities. Unlike the GDPR, which encompasses both digital and manual data, the DPDP Act is confined to **digital personal data**, whether collected online or later digitised. This narrower scope simplifies compliance but excludes large volumes of offline data from protection.

The Act's framework is **consent-centric**, requiring that consent be free, informed, specific, and unambiguous. However, it introduces the concept of **"deemed consent"**, permitting data processing without explicit approval in cases such as government functions, compliance with legal obligations, or emergencies, provisions far broader than those under the GDPR or LGPD.

While the DPDP Act grants certain rights to individuals such as access, correction, erasure, and grievance redressal.[35] It notably omits others like **data portability** and the **right to object to processing**, both of which are guaranteed under the GDPR and LGPD. The creation of the **Data Protection Board of India (DPBI)** represents an institutional advancement, yet its independence remains questionable since members are appointed and removable by the Central Government.

In contrast, the **GDPR's supervisory authorities** and Brazil's **ANPD** enjoy operational autonomy, ensuring impartial enforcement. Moreover, India's broad **governmental exemptions under Section 17**[36], which allow the state to exempt any agency from compliance on grounds of sovereignty, security, or public order raise serious concerns about potential surveillance and erosion of privacy protections.

Finally, while the GDPR mandates stringent **cross-border data transfer restrictions** based on adequacy principles, India's DPDP Act leaves this to government notification, allowing transfers only to countries approved by the Central Government.[37] This lack of clarity may impede India's prospects for **EU adequacy recognition**[38], an important factor for global trade and data flows.

---

[35] "Digital Personal Data Protection Act, 2023 – Key Highlights," *azb available at*: https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/.
[36] Digital Personal Data Protection Act, 2023
[37] Taxmann, "Cross-Border Data Transfers under the DPDP Act 2023" *Taxmann Blog*, 2025*available at*: https://www.taxmann.com/post/blog/cross-border-data-transfers-under-the-dpdp-act/
[38] Kevin Yun , "EU Adequacy Decisions: Data Protection Standards for Cross-Border Transfers" *Complydog.com*, 2018*available at*: https://complydog.com/blog/adequacy-decisions.

4.6 Comparative Observations and Global Positioning

Philosophically, the GDPR and LGPD are founded on **privacy as a human right**, while the CCPA approaches data protection through the lens of **consumer empowerment**. India's DPDP Act occupies a middle ground—anchored in the constitutional recognition of privacy yet operationalised through a **state-controlled and administratively flexible framework**.

Institutionally, India lags behind the GDPR and LGPD in ensuring **regulatory independence**. The concentration of power within the executive branch could hinder effective enforcement and public trust. In contrast, the European and Brazilian models demonstrate the importance of autonomous data protection authorities in maintaining checks and balances.

Substantively, India's regime is less comprehensive. It omits manual data, offers a limited set of user rights, and allows wide state exemptions. Although the CCPA is also narrower in scope, its enforcement mechanisms are clearer and its remedies more accessible to consumers.[39]

Despite these shortcomings, the DPDP Act provides a strong foundation for future reform. It reflects a realistic attempt to align India's privacy framework with global standards while accommodating the nation's developmental priorities and digital expansion. The Act's success will depend on the **complementing DPDP Rules, 2025**[40], and how courts interpret the balance between privacy and public interest in its application.

5.Challenges in India's Data Protection Ecosystem

Despite the enactment of the Digital Personal Data Protection Act, 2023, India continues to face significant challenges in operationalising a robust, rights-based, and technologically adaptive data protection framework. These challenges span across various dimensions, highlighting the complexities of enforcing privacy in a nation as diverse and digitally vast as India.

[39] Ben Dooley, "A Comparative Analysis of Data Privacy Laws: GDPR, CCPA, LGPD, PDPA, and Privacy Act" *Linkedin.com*, 2023*available at*: https://www.linkedin.com/pulse/comparative-analysis-data-privacy-laws-gdpr-ccpa-lgpd-ben-dooley/

[40] Sarah Abraham, "Law & the Digital Society: Fine-tuning Digital Personal Data Protection Rules 2025 for Effective Implementation" *Thehinducentre.com*, 2025*available at*: https://www.thehinducentre.com/the-arena/current-issues/law-the-digital-society-fine-tuning-digital-personal-data-protection-rules-2025-for-effective-implementation/article69284580.ece

5.1 Institutional and Enforcement Deficiencies

A fundamental concern lies in the lack of an independent enforcement authority. The Data Protection Board of India (DPBI), constituted under the DPDP Act, is empowered to inquire into data breaches and impose penalties. However, the Board's structural dependence on the Central Government for appointments, composition, and functions raises apprehensions about its autonomy.[41]Without institutional independence, enforcement risks becoming inconsistent and politically influenced. This stands in contrast to the European Data Protection Board (EDPB) under the GDPR, which functions as an independent supervisory authority insulated from governmental control. The absence of a decentralised network of regional authorities also limits accessibility and responsiveness, especially in addressing grievances from India's vast population.

5.2 Broad Governmental Exemptions and Surveillance Concerns

Section 17 of the DPDP Act grants the Central Government wide discretion to exempt State agencies from compliance with core data protection principles for reasons such as national security, sovereignty, and public order. While national interest considerations are legitimate, the provision's lack of procedural safeguards or judicial oversight renders it susceptible to misuse. In a country where state surveillance practices have been criticised for opacity and overreach, such unchecked exemptions threaten to dilute the very privacy guarantees recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).[42] The absence of an independent mechanism to review surveillance authorisations further compounds the risk of arbitrary intrusion into citizens' data.

5.3 Absence of Comprehensive Data Subject Rights

Although the DPDP Act introduces key data principal rights such as access, correction, and erasure, it omits certain internationally recognised rights, including data portability, the right to object to processing, and the right to be forgotten in its broader form. The absence of these rights restricts individuals from exercising meaningful control over their personal information.

[41] "India's Data Privacy Law - Understanding DPDP Act, challenges and opportunities in the space - UNLEASH Capital Partners, Inc.," *UNLEASH Capital Partners, Inc.*, 2024*available at*: https://unleashcp.com/blog/DataPrivacy

[42] "The Politics of India's Data Protection Ecosystem," *Economic and Political Weekly*, 2019*available at*: https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem

Additionally, the limited scope for consent withdrawal and lack of transparency obligations on data fiduciaries hinder the formation of a truly rights-based privacy regime. In contrast, frameworks like the GDPR and Brazil's LGPD ensure a more holistic set of user rights, enabling data subjects to participate actively in data governance and take control of their personal data.[43]

5.4 Technological and Infrastructural Limitations

Effective data protection requires not only legal standards but also technological readiness. India faces considerable infrastructural challenges in terms of cybersecurity preparedness, data localisation capabilities, and capacity for secure storage and processing. Small and medium enterprises (SMEs), which form a large part of India's digital economy, often lack resources to implement sophisticated compliance mechanisms. Furthermore, there exists a significant digital literacy gap among users, which undermines informed consent and increases vulnerability to misuse. The absence of clear standards also impedes compliance efficiency across sectors.

5.5 Ambiguity in Cross-Border Data Transfer Mechanisms

The DPDP Act adopts a flexible yet opaque framework for cross-border data transfers, allowing the government to specify countries or territories where such transfers are permitted. However, the lack of transparent criteria for these decisions raises uncertainty for multinational corporations and technology firms operating in India. Without predictable adequacy standards akin to those under the GDPR, India risks creating a fragmented data transfer regime that could affect global business operations and impede foreign investment.[44]

5.6 Need for Sectoral Integration and Harmonisation

India's data protection landscape continues to be fragmented, with sector-specific regulations such as those under the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), and Insurance Regulatory and Development Authority of India (IRDAI) operating

[43] Ben Dooley, "A Comparative Analysis of Data Privacy Laws: GDPR, CCPA, LGPD, PDPA, and Privacy Act" *Linkedin.com*, 2023*available at*: https://www.linkedin.com/pulse/comparative-analysis-data-privacy-laws-gdpr-ccpa-lgpd-ben-dooley/

[44] "DPDP Rules, 2025: Significant Data Fiduciaries and Data Transfers," *Software Freedom Law Center, India • Defender of Your Digital Freedom*, 2025*available at*: https://sflc.in/dpdp-rules-2025-significant-data-fiduciaries-and-data-transfers/

independently. The absence of a harmonised approach leads to regulatory overlaps and compliance burdens. A unified framework integrating data protection principles across sectors is essential to ensure consistency, reduce ambiguity, and promote trust among stakeholders.

6.The Way Forward: Recommendations for Strengthening India's Data Protection Regime

The enactment of the **Digital Personal Data Protection Act, 2023 (DPDP Act)** is a landmark achievement, reflecting India's growing recognition of privacy as a fundamental right and its intent to align with global data governance standards. However, as with any nascent framework, its success depends not merely on statutory articulation but on effective implementation, institutional integrity, and continued reform. Strengthening India's data protection legislation requires addressing key challenges ranging from institutional independence to user empowerment, technological readiness, and international interoperability through a comprehensive and forward-looking approach.

A central reform lies in ensuring the **independence and accountability of the Data Protection Board of India (DPBI)**. The Board, as the primary enforcement authority, must function free from executive influence to maintain public confidence and uphold the rule of law.[45] Drawing lessons from the **European Data Protection Board (EDPB)** under the GDPR, India should adopt a **collegiate model** of governance comprising members from diverse professional and regional backgrounds, thereby ensuring impartiality and transparency. Regular parliamentary oversight, public disclosure of decisions, and the establishment of regional branches would further democratise enforcement and make data protection more accessible across India's vast geography.

Another critical reform area concerns **broad governmental exemptions** under Section 17 of the DPDP Act. While national security and sovereignty are legitimate state interests, this provision risks undermining the constitutional guarantee of informational privacy recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). These exemptions must therefore be **narrowed and subjected to procedural safeguards**, including judicial or independent review. A dedicated **surveillance framework**, under parliamentary supervision, could ensure

[45] Amal Chandra C., "Strengthening India's Cybersecurity and Data Privacy Landscape: A Comprehensive Overview," 70 *Indian Journal of Public Administration* 466–78 (2024).

that data access by state agencies adheres to the principles of legality, necessity, and proportionality, preventing arbitrary or disproportionate intrusions into personal data.

India's current framework also requires a **broader recognition of data subject rights** to strengthen user autonomy and align with international standards. While the DPDP Act grants rights to access, correction, and erasure, it omits essential rights such as **data portability, the right to object to processing**, and a comprehensive **right to be forgotten**. Incorporating these provisions would enable individuals to exercise greater control over their digital identities. Moreover, operational clarity on how these rights can be invoked along with specific timelines and grievance redress mechanisms should be detailed through subordinate legislation. Parallelly, **digital literacy initiatives** and **public awareness campaigns** are a necessity to ensure that these rights are understood and effectively exercised by all citizens, including those in rural and marginalised communities.

Equally vital is embedding **privacy by design** into India's digital ecosystem. Organisations, particularly significant data fiduciaries, should be legally obligated to integrate privacy principles into their operational architecture. Mandatory **Data Protection Impact Assessments (DPIAs)** should become standard practice. This proactive approach not only ensures compliance but also cultivates a culture of ethical data governance.

Given India's role in the global digital economy, it is imperative to establish **clear and predictable cross-border data transfer mechanisms**. The current model, which empowers the government to designate countries for data transfer without specifying objective criteria, introduces uncertainty for global businesses. India should develop **transparent standards**, similar to the GDPR's adequacy decisions, to evaluate foreign jurisdictions based on reciprocal privacy guarantees. Simultaneously, promoting **secure and scalable data localisation infrastructure** would enhance national resilience without compromising international cooperation. Balancing these dimensions will be key to maintaining investor confidence while safeguarding citizens' data.

From an infrastructural standpoint, India's data protection success hinges on **technological capacity and cybersecurity readiness**. Many small and medium enterprises (SMEs) lack the expertise and resources to comply with the DPDP Act's obligations effectively. The government should therefore establish **compliance facilitation frameworks**, providing technical guidance and subsidies for privacy infrastructure. Developing **sector-specific**

standards for high-risk industries such as finance, healthcare, and education can help tailor obligations proportionately. Strengthening **cybersecurity infrastructure**, fostering **public-private partnerships**, and supporting **privacy-oriented innovation** will ensure that India's digital transformation remains secure, inclusive, and sustainable.

Additionally, to overcome the current regulatory fragmentation, India needs a **coordinated and harmonised approach** across its federal and sectoral landscape. Various regulators currently enforce sector-specific privacy norms, often resulting in overlap or inconsistency. The establishment of **a centralised council** could serve as a unifying platform to harmonise standards. Integrating state-level authorities into this network would further support decentralised and uniform implementation across India's diverse administrative framework.

In essence, the way forward for India's data protection framework lies in a **balanced, multi-dimensional strategy**, one that combines legal obligations, institutional autonomy, technological advancement, and citizen empowerment. The **Digital Personal Data Protection Act, 2023** has laid a crucial foundation, but it's true potential will be realised only through continued legislative evolution. India must strive to build a **privacy-respecting digital culture**, grounded in transparency, accountability, and constitutional morality. By reinforcing institutional independence, enhancing data subject rights, promoting privacy by design, and ensuring global compatibility, India can develop a data protection framework that not only safeguards individual liberty but also strengthens its position as a trusted global digital leader.

9. Conclusion

The evolution of India's data protection framework reflects a narrative of constitutional maturation, technological transformation, and societal awakening to the value of informational privacy. From the limited provisions of the **Information Technology Act, 2000**, to the constitutional recognition of privacy in *Justice K.S. Puttaswamy (Retd.) v. Union of India* **(2017)**, India's legal trajectory underscores a gradual yet decisive shift towards a rights-based approach to data governance. The enactment of the **Digital Personal Data Protection Act, 2023** signifies a historic legislative response to the challenges posed by the digital age.

The DPDP Act represents not the culmination but the **commencement of India's privacy journey**. Its success depends on the effectiveness of its implementation, the independence of its enforcement institutions, and the precision of its subordinate legislation. The Act's

simplified, consent-centric model introduces much-needed structure to India's fragmented regime but still falls short of the comprehensive safeguards seen in global standards like the **General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA)**, and **Brazil's Lei Geral de Proteção de Dados (LGPD)**. Key gaps such as broad governmental exemptions, limited individual rights, and insufficient procedural clarity must be addressed through legislative refinement and policy reform to ensure that privacy protection is not merely symbolic, but substantive and enforceable.

India's data protection landscape also faces **structural and infrastructural challenges** ranging from technological limitations and low digital literacy to inconsistent regulatory coordination across sectors. Bridging these gaps requires sustained investment in cybersecurity capacity, institutional transparency, and digital awareness. Moreover, developing a **culture of privacy** one that treats data protection as intrinsic to dignity and democracy will be vital in ensuring long-term success.

Ultimately, India stands at a pivotal juncture where law, technology, and constitutional morality converge. The **Digital Personal Data Protection Act, 2023**, if implemented the right way, has the potential to position India as a **global leader in data governance** as one that protects individual rights while nurturing digital innovation. The path forward must rest on ensuring that the right to privacy is not a privilege reserved for the few but a guaranteed protection for all. In doing so, India can transform its data protection regime into a model that is not only legally sound and technologically adaptive but also **deeply anchored in the constitutional promise of liberty and human dignity**.