GROUND REALITY OF INDIA'S DATA PROTECTION REGIME: COMPLIANCE CHALLENGES AFTER THE DPDP RULES, 2025

Rakshit Sharma, Amity University, Noida

ABSTRACT

This paper examines the ground reality of India's data protection regime following the enactment of the Digital Personal Data Protection Act, 2023 and the subsequent introduction of the Digital Personal Data Protection Rules, 2025. While the Act establishes a formal legal framework for regulating personal data, the Rules aim to operationalise its provisions by detailing compliance requirements and procedural mechanisms. However, the effectiveness of this framework depends not only on its legal design but also on its practical implementation.

The study adopts a doctrinal and analytical approach, supplemented by an examination of recent policy developments and empirical trends in India's digital ecosystem. It focuses on the compliance obligations imposed on data fiduciaries and evaluates the challenges faced by organizations, regulators, and users in adapting to the new regime.

The findings indicate that despite the introduction of structured compliance mechanisms, significant challenges persist. These include regulatory ambiguity, high compliance costs, technological limitations, evolving enforcement capacity, and low levels of digital literacy among users. The paper further highlights that the scale and diversity of India's digital environment complicate uniform implementation, resulting in inconsistencies in compliance.

The study argues that the current framework reflects a compliance-oriented model that emphasizes procedural adherence over substantive protection. As a result, a gap continues to exist between regulatory intent and ground-level enforcement.

The paper concludes that while the DPDP Act and Rules represent an important step towards data governance in India, their success depends on strengthening institutional capacity, clarifying regulatory standards, enhancing public awareness, and aligning legal provisions with practical realities.

Keywords: Data Fiduciaries, Regulatory Ambiguity, Institutional Capacity, Data Governance, Privacy Compliance

Introduction

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marked a significant milestone in India's journey towards establishing a comprehensive legal framework for the protection of personal data. Prior to this legislation, data protection in India was governed by fragmented provisions under the Information Technology Act, 2000, which were inadequate to address the complexities of the digital economy.[1]

In order to operationalise the provisions of the DPDP Act, the Government of India introduced the Digital Personal Data Protection Rules, 2025 (DPDP Rules). These Rules aim to provide procedural clarity regarding compliance requirements, including consent mechanisms, data breach reporting, grievance redressal, and obligations of data fiduciaries.[2]

While the Act and the Rules together create a structured framework for data governance, their effectiveness depends not merely on legislative design but on their practical implementation in real-world conditions. In a country like India, characterised by a vast digital population, varying levels of technological capacity, and significant socio-economic diversity, the transition from legal framework to effective compliance presents considerable challenges.

Recent developments indicate that India has witnessed a rapid expansion of its digital ecosystem, with increasing internet penetration and widespread adoption of digital services.[3] However, this growth has been accompanied by rising concerns regarding data breaches, cybersecurity threats, and misuse of personal data, highlighting the need for robust and enforceable data protection mechanisms.

Despite the introduction of detailed compliance obligations under the DPDP Rules, organizations particularly small and medium enterprises face difficulties in adapting to the regulatory requirements due to cost constraints, lack of technical expertise, and uncertainty in

[1] Information Technology Act, 2000, § 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[2] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (Government of India, 2025).
[3] Ministry of Electronics and Information Technology, India Digital Economy Report 2025 (Government of India, 2025).

interpreting legal provisions.[4] At the same time, users often lack awareness of their data protection rights, which undermines the effectiveness of consent-based frameworks.

Furthermore, the enforcement architecture under the Act is still evolving, with questions surrounding institutional capacity, regulatory clarity, and consistency in adjudication. These factors contribute to a gap between regulatory intent and ground-level implementation, raising concerns about the practical effectiveness of India's data protection regime.

This paper seeks to examine the ground reality of compliance under the DPDP Act and Rules, focusing on the challenges faced by stakeholders in implementing the law. It argues that while the legal framework represents a significant step forward, its success is constrained by structural, technological, and socio-economic limitations that affect compliance in practice.

Overview of the DPDP Act, 2023 and DPDP Rules, 2025

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive attempt to establish a unified legal framework governing the processing of personal data. The Act seeks to regulate the collection, storage, and use of digital personal data by both private entities and the State, while balancing the need for economic development with the protection of individual privacy.[5]

At its core, the Act introduces a structured framework based on key concepts such as data principals, data fiduciaries, and consent-based processing. A data principal refers to the individual to whom the personal data relates, while a data fiduciary is the entity that determines the purpose and means of processing such data.[6] The use of the term "*fiduciary*" reflects an expectation of trust and responsibility in handling personal data.

The Act primarily relies on consent as the legal basis for processing, requiring that consent be free, specific, informed, unconditional, and unambiguous.[7] It also recognises certain exceptions in the form of "*legitimate uses*," where data may be processed without consent under specified circumstances, including state functions and legal obligations.

In addition to establishing obligations for data fiduciaries, the Act provides certain rights to data principals, including the right to access information, the right to correction and erasure,

[4] Federation of Indian Chambers of Commerce and Industry (FICCI), Data Protection and Privacy in India: Industry Report (2024).
[5] Digital Personal Data Protection Act, 2023 (India).
[6] Ibid.
[7] Ibid.

and the right to grievance redressal.[8] However, as discussed in later sections, the scope of these rights remains relatively limited compared to international standards.

The enforcement of the Act is entrusted to the Data Protection Board of India, which is empowered to adjudicate disputes and impose monetary penalties in cases of non-compliance.[9] The Act adopts a penalty-based enforcement mechanism, with significant financial penalties aimed at ensuring adherence to its provisions.

While the DPDP Act lays down the substantive legal framework, the Digital Personal Data Protection Rules, 2025 play a crucial role in operationalising its provisions. These Rules provide procedural clarity and detail regarding the implementation of compliance requirements.

The DPDP Rules, 2025 elaborate on several key aspects, including:

- the format and manner of obtaining consent
- requirements for privacy notices
- procedures for reporting personal data breaches
- mechanisms for grievance redressal
- obligations of significant data fiduciaries

The Rules also introduce greater specificity in relation to compliance processes, thereby reducing some of the ambiguity present in the parent legislation.[10] However, they simultaneously introduce new layers of operational complexity for organizations.

Importantly, the Rules reflect a shift from legislative principles to practical enforcement, translating broad statutory obligations into actionable compliance requirements. This transition highlights the increasing importance of procedural mechanisms in ensuring data protection.

Despite these developments, the combined framework of the Act and the Rules continues to raise questions regarding its practical feasibility. The detailed compliance requirements, while necessary for effective regulation, may impose significant burdens on organizations, particularly those with limited resources.

[8] Ibid.
[9] Ibid.
[10] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (Government of India, 2025).

Thus, while the DPDP Act, 2023 and the DPDP Rules, 2025 together establish a structured and evolving data protection regime, their real impact depends on how effectively these provisions are implemented in practice. This sets the stage for a closer examination of the compliance framework and the challenges associated with it.

Compliance Framework under the DPDP Rules, 2025

The Digital Personal Data Protection Rules, 2025 play a critical role in translating the broad principles of the Digital Personal Data Protection Act, 2023 into practical compliance obligations. While the Act establishes the legal foundation, the Rules provide the procedural and operational framework necessary for implementation.

A central feature of the compliance framework is the requirement for valid consent mechanisms. Data fiduciaries are required to obtain consent through clear and accessible notices that specify the purpose of data processing, the nature of personal data being collected, and the rights available to the data principal.[11] The Rules emphasise that such notices must be presented in a manner that is understandable and accessible, reflecting an attempt to enhance transparency.

In addition to consent, the Rules impose obligations relating to data breach reporting. Data fiduciaries are required to notify the relevant authorities and affected individuals in the event of a personal data breach.[12] This requirement is intended to ensure accountability and enable timely remedial action. However, it also places significant responsibility on organizations to detect and report breaches promptly.

Another important aspect of the compliance framework is the establishment of grievance redressal mechanisms. Data fiduciaries must provide accessible channels through which data principals can raise complaints regarding the processing of their personal data.[13] The Rules further require that such grievances be addressed within a specified timeframe, thereby introducing a degree of procedural accountability.

The Rules also recognise the role of consent managers, who act as intermediaries to facilitate the giving, managing, and withdrawal of consent.[14] This reflects an innovative approach aimed at simplifying user interaction with data protection mechanisms. However, the operational

[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Ibid.

effectiveness of consent managers depends on their design, accountability, and integration within the broader regulatory framework.

Further, additional compliance obligations are imposed on Significant Data Fiduciaries, which may include:

- appointment of a Data Protection Officer
- implementation of risk assessment measures
- periodic audits and compliance reviews[15]

These enhanced requirements are intended to ensure stricter regulation of entities that process large volumes of data or pose higher risks to individuals.

While the compliance framework under the DPDP Rules, 2025 provides much-needed clarity, it also introduces a layer of operational complexity. Organizations are required to integrate legal requirements into their technical and administrative processes, which may involve significant restructuring of data management systems.

Moreover, the framework places considerable emphasis on procedural compliance, focusing on the fulfilment of formal requirements such as notices, documentation, and reporting. While these measures are essential, they do not necessarily guarantee substantive protection of personal data.

Thus, the compliance framework under the DPDP Rules, 2025 represents a structured attempt to operationalise data protection law in India. However, its effectiveness depends on the ability of organizations, regulators, and users to adapt to these requirements in practice. This raises important questions regarding the challenges faced in achieving meaningful compliance, which are examined in the following section.

Key Compliance Challenges

Regulatory Ambiguity and Interpretational Uncertainty

Despite the introduction of the Digital Personal Data Protection Rules, 2025, a significant challenge in achieving effective compliance lies in the ambiguity and lack of clarity in key regulatory provisions. While the Rules attempt to operationalise the Digital Personal Data

[15] Ibid.

Protection Act, 2023, several concepts remain open-ended and subject to varying interpretations.

One of the primary areas of concern is the continued use of broad and undefined terms, such as "*reasonable security safeguards*" and "*legitimate use*." The absence of precise definitions or detailed standards makes it difficult for organizations to determine the exact scope of their compliance obligations.[16] This uncertainty often results in inconsistent implementation across sectors.

Further, while the Rules provide procedural guidance, they do not fully resolve questions relating to:

- the level of security required
- acceptable standards for data retention
- thresholds for determining risk

This creates a situation where organizations must rely on internal interpretation or external advisory, leading to variation in compliance practices.

Regulatory ambiguity also increases the risk of over-compliance or under-compliance. Some organizations may adopt excessively stringent measures to avoid penalties, thereby increasing operational costs, while others may interpret the provisions narrowly, resulting in inadequate data protection.

From a legal perspective, such ambiguity undermines the principle of legal certainty, which requires laws to be clear, predictable, and capable of consistent application. Scholars have argued that vague regulatory standards in data protection law can lead to increased discretion on the part of enforcement authorities, thereby affecting fairness and uniformity.[17]

Another important issue is the evolving nature of the regulatory framework itself. As the DPDP Rules, 2025 are still in the early stages of implementation, organizations face uncertainty regarding future amendments, interpretational guidance, and enforcement trends. This transitional phase complicates long-term compliance planning.

[16] Digital Personal Data Protection Act, 2023 (India); Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (Government of India, 2025).
[17] Cary Coglianese, "Measuring Regulatory Performance: Evaluating the Impact of Regulation and Regulatory Policy" (2012) 36 OECD Publishing.

Industry analyses have also highlighted that businesses in India are currently navigating a fluid regulatory environment, where formal legal requirements are still being supplemented by policy guidance and emerging best practices.[18] This lack of stability further contributes to compliance challenges.

Moreover, in the absence of sector-specific guidelines, organizations operating in industries such as fintech, healthcare, and e-commerce must interpret general provisions in highly specialized contexts. This increases the complexity of compliance and raises the risk of inconsistent standards across sectors.

Thus, regulatory ambiguity and interpretational uncertainty constitute a significant barrier to effective compliance under the DPDP Act and Rules. Without clearer definitions, detailed guidelines, and consistent regulatory interpretation, organizations may struggle to align their practices with legal requirements.

Cost and Resource Constraints

A major challenge in the implementation of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 is the financial and operational burden of compliance, particularly for small and medium enterprises (SMEs) and startups.

The compliance framework requires organizations to establish:

- data protection policies
- consent management systems
- grievance redressal mechanisms
- cybersecurity safeguards
- internal monitoring and reporting processes

While these measures are necessary to ensure data protection, they involve significant financial and technical investment.[19] Larger corporations may have the resources to implement such systems effectively, but smaller entities often lack the necessary infrastructure and expertise.

One of the key concerns is the disproportionate impact of compliance costs. SMEs form a

[18] NASSCOM, India Data Protection Landscape Report 2025 (2025).
[19] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (Government of India, 2025).

substantial part of India's digital economy, yet they may not have access to dedicated legal teams, data protection officers, or advanced cybersecurity tools. As a result, compliance may become a resource-intensive exercise, diverting attention from core business operations.

Reports indicate that regulatory compliance costs in emerging data protection regimes can act as a barrier to entry, particularly for startups operating in competitive digital markets.[20] This may hinder innovation and reduce the growth potential of new enterprises.

Further, organizations are required to invest in technical upgrades and training, including:

- secure data storage systems
- encryption technologies
- employee awareness programs

Such investments are not one-time costs but require continuous updating and maintenance, especially in light of evolving cyber threats and technological advancements.

Another challenge is the shortage of skilled professionals in the field of data protection and cybersecurity. Organizations may face difficulty in hiring qualified personnel capable of managing compliance requirements, thereby increasing reliance on external consultants and raising operational costs.[21]

Additionally, compliance obligations may vary depending on whether an entity is classified as a Significant Data Fiduciary, which entails stricter requirements such as audits and impact assessments. This creates further complexity and cost implications for organizations operating at scale.

From a policy perspective, while strict compliance requirements are essential for protecting personal data, they must be balanced against the need to support economic growth and innovation. Overly burdensome compliance frameworks may discourage participation in the digital economy, particularly among smaller entities.

Thus, the financial and resource constraints associated with compliance under the DPDP Act and Rules represent a significant challenge, affecting the ability of organizations to implement data protection measures effectively.

[20] World Bank, World Development Report 2021: Data for Better Lives (World Bank 2021).
[21] International Labour Organization, Skills Demand in Cybersecurity and Data Protection Roles in Asia (2024).

Technological Challenges

The implementation of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 is significantly affected by technological challenges, particularly in the context of India's rapidly evolving digital ecosystem. While the legal framework imposes obligations relating to data security and processing, the technological capacity required to meet these standards is not uniformly available across organizations.

One of the primary challenges arises from the increasing complexity of data processing technologies, including artificial intelligence (AI), machine learning, and big data analytics. These technologies enable large-scale collection and automated processing of personal data, often in ways that are difficult to monitor or regulate.[22] As a result, ensuring compliance with principles such as purpose limitation and data minimization becomes technically challenging.

Further, the use of automated decision-making systems raises concerns regarding transparency and accountability. Many AI-driven systems operate as "black boxes," making it difficult for organizations to explain how personal data is processed or how decisions are made. This creates practical difficulties in meeting obligations related to transparency and user awareness.

Another significant issue is the increasing frequency and sophistication of cyber threats. India has witnessed a substantial rise in data breaches, ransomware attacks, and cyber intrusions in recent years.[23] Organizations are required to implement "reasonable security safeguards," but the lack of clear technical standards makes it difficult to determine what level of protection is sufficient.

In addition, the uneven distribution of technological infrastructure across sectors and regions further complicates compliance. While large corporations may have access to advanced cybersecurity systems and cloud infrastructure, smaller entities often rely on basic or outdated systems, increasing their vulnerability to data breaches.

The challenge is compounded by the need for continuous technological adaptation. Data protection is not a one-time compliance requirement but an ongoing process that requires regular updates to security systems, monitoring mechanisms, and risk assessment practices. This dynamic nature of compliance places additional strain on organizational resources.

[22] NITI Aayog, National Strategy for Artificial Intelligence: Responsible AI for All (updated policy discussions 2024).
[23] Indian Computer Emergency Response Team (CERT-In), Annual Cyber Security Incidents Report 2025.

Another important concern is the integration of legal and technological frameworks. Effective compliance requires coordination between legal teams, IT professionals, and management. However, many organizations lack the interdisciplinary capacity to align legal requirements with technological implementation, resulting in gaps in compliance.

Recent policy analyses have highlighted that developing countries, including India, face structural challenges in aligning data governance frameworks with technological capabilities, particularly in high-growth digital environments.[24] This mismatch between legal expectations and technological capacity creates practical barriers to effective enforcement.

Thus, technological challenges play a critical role in shaping the ground reality of compliance under the DPDP Act and Rules. Without adequate technological infrastructure, expertise, and standardisation, the implementation of data protection obligations remains inconsistent and difficult to achieve.

Enforcement and Institutional Limitations

The effectiveness of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 ultimately depends on the strength and efficiency of the enforcement mechanism, which, in the Indian context, is still in a developing stage.

The Act establishes the Data Protection Board of India as the primary authority responsible for adjudication and enforcement. However, the practical functioning of this body raises several concerns relating to institutional capacity, procedural clarity, and operational readiness.[25]

One of the key challenges is the limited institutional capacity to handle the scale of data protection issues in India. With millions of digital users and organizations processing personal data, the volume of potential complaints, breaches, and compliance issues is likely to be substantial. In such a scenario, the ability of a single regulatory body to effectively manage enforcement becomes questionable.

Further, the enforcement framework lacks detailed procedural guidelines, particularly with respect to:

- investigation processes
- evidentiary standards

[24] United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2024.
[25] Digital Personal Data Protection Act, 2023 (India).

- timelines for adjudication

This absence of clarity may result in delays, inconsistent decision-making, and uncertainty for stakeholders.

Another significant concern is the evolving nature of the regulatory framework. As the DPDP Rules, 2025 are still in the early stages of implementation, enforcement practices are yet to stabilise. Organizations are therefore required to operate in an environment where regulatory expectations are still developing, making compliance more complex.

Additionally, the effectiveness of enforcement is closely linked to the availability of technical expertise and resources within regulatory institutions. Data protection enforcement requires not only legal knowledge but also an understanding of cybersecurity, data systems, and digital technologies. Reports indicate that many regulatory bodies in emerging economies face challenges in building such multidisciplinary capacity.[26]

The issue is further compounded by the increasing scale of cyber incidents and data breaches. As digital adoption grows, the number of enforcement cases is likely to increase, placing additional pressure on institutional resources. Without adequate infrastructure and personnel, enforcement may become reactive rather than proactive.

Another important aspect is the limited clarity regarding coordination with other regulatory bodies. In sectors such as finance, telecommunications, and e-commerce, multiple regulators may have overlapping jurisdiction. The absence of a clearly defined framework for inter-agency coordination may lead to regulatory fragmentation and inefficiency.

Moreover, the credibility of enforcement mechanisms depends on transparency and consistency. The lack of publicly available guidelines, precedents, and standardized procedures may reduce predictability in enforcement outcomes, thereby affecting compliance behaviour.

From a broader perspective, regulatory effectiveness requires not only formal authority but also institutional legitimacy and public trust. If enforcement mechanisms are perceived as inconsistent or insufficiently independent, their deterrent effect may be weakened.

Thus, while the DPDP Act and Rules establish a formal enforcement structure, the ground reality reflects a system that is still evolving, facing significant challenges in terms of capacity,

[26] Asian Development Bank, Regulating the Digital Economy in Asia: Institutional Challenges and Capacity Building (2024).

clarity, and coordination. These institutional limitations constitute a major barrier to achieving effective data protection in practice.

User Behaviour and Consent Fatigue

A critical yet often overlooked challenge in the implementation of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 relates to user behaviour, particularly the phenomenon of consent fatigue. While the legal framework is built on the premise of informed and voluntary consent, the practical realities of user interaction with digital systems raise serious concerns about its effectiveness.

The compliance framework requires data fiduciaries to obtain consent through notices that inform users about the nature and purpose of data processing. However, in practice, users are frequently presented with lengthy and complex privacy policies, which they tend to accept without reading or fully understanding.[27] This behaviour reduces consent to a mere formality rather than a meaningful exercise of choice.

The problem is exacerbated in India due to low levels of digital literacy and awareness. A significant portion of users may lack the knowledge required to interpret privacy notices or understand the implications of data sharing. As a result, consent is often given without genuine comprehension, undermining the foundational principle of the data protection regime.

Another important factor is the imbalance of power between users and service providers. In many cases, access to essential digital services such as social media platforms, financial services, and e-commerce requires users to accept terms and conditions. This creates a situation where consent is not entirely voluntary but is instead driven by necessity, raising questions about its validity.

Scholarly research has highlighted that traditional models of consent are increasingly ineffective in complex digital environments. Users are often faced with repeated consent requests across multiple platforms, leading to fatigue and disengagement.[28] This phenomenon weakens the regulatory framework, as it assumes a level of user engagement that does not exist in practice.

Further, the DPDP Rules, 2025 introduce mechanisms such as consent managers, which are

[27] Competition Commission of India, Market Study on the Telecom Sector in India (2021).
[28] Neil M. Richards & Woodrow Hartzog, "The Pathologies of Digital Consent" (2019) 96 Washington University Law Review 1461.

intended to simplify the process of managing consent. However, the effectiveness of such mechanisms depends on their adoption, usability, and integration into digital ecosystems. Without widespread implementation and user awareness, these tools may have limited impact.

Additionally, behavioural patterns indicate that users tend to prioritise convenience over privacy, particularly in fast-paced digital environments. This tendency further reduces the likelihood of informed decision-making and weakens the protective function of consent-based regulation.

From a policy perspective, reliance on consent as the primary basis for data processing may be insufficient in addressing modern data protection challenges. Effective regulation requires not only user consent but also strong accountability mechanisms and structural safeguards that operate independently of user behaviour.

Thus, user behaviour and consent fatigue represent a fundamental challenge to the practical implementation of the DPDP Act and Rules. The gap between the theoretical model of informed consent and actual user practices highlights the limitations of a consent-centric approach to data protection.

Cross Border and Global Compliance Issues

In an increasingly interconnected digital economy, the regulation of cross-border data transfers presents a significant challenge for the effective implementation of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025. While the framework permits international data transfers to jurisdictions notified by the Central Government, it does not provide a detailed or transparent mechanism for determining such jurisdictions.

This lack of clarity creates uncertainty for organizations, particularly those operating across multiple jurisdictions. Multinational companies are required to navigate divergent data protection regimes, each with its own compliance requirements.[29] In the absence of a structured framework for cross-border transfers, organizations may face difficulties in aligning their practices with both Indian law and international standards.

A key issue is the absence of clearly defined adequacy criteria or equivalent safeguards. In many global frameworks, cross-border transfers are permitted only when the receiving jurisdiction ensures an adequate level of data protection. The DPDP framework, however,

[29] Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013).

relies on executive discretion without specifying objective standards, which may result in inconsistent or unpredictable decisions.

This creates compliance challenges for organizations that rely on global data flows, such as:

- cloud service providers
- financial institutions
- e-commerce platforms

These entities often process data across multiple countries, making it essential to have clear and consistent regulatory standards.

Further, the absence of mechanisms such as:

- standard contractual clauses
- binding corporate rules
- structured risk assessments

limits the ability of organizations to implement internally consistent compliance frameworks. Without such tools, companies may struggle to ensure that data transferred outside India remains adequately protected.

Another important concern is the potential impact on international trade and digital economy participation. Uncertainty in data transfer regulations may discourage foreign investment and complicate cross-border business operations. Studies have shown that predictable and transparent data governance frameworks are essential for fostering global digital trade.[30]

Additionally, conflicts may arise between Indian regulations and foreign laws, particularly in jurisdictions with stricter data protection standards. Organizations may face situations where compliance with one legal system leads to non-compliance with another, creating legal and operational risks.

From a policy perspective, effective regulation of cross-border data flows requires a balance between data protection and economic integration. Overly restrictive or unclear frameworks may hinder innovation and global collaboration, while overly permissive approaches may

[30] World Trade Organization, World Trade Report 2023: Re-globalization for a Secure, Inclusive and Sustainable Future (2023).

compromise privacy protections.

Thus, the lack of a clear, structured, and transparent framework for cross-border data transfers under the DPDP Act and Rules represents a significant compliance challenge. It highlights the need for greater regulatory clarity and alignment with international standards.

Ground Reality and Emerging Trends

The practical implementation of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 must be assessed in light of the current trends in India's digital ecosystem, which reveal significant challenges in achieving effective compliance.

India has witnessed a rapid expansion in digital adoption, with internet penetration reaching hundreds of millions of users and digital services becoming integral to everyday life.[31] This growth has led to an unprecedented increase in the volume of personal data being generated, collected, and processed across sectors such as finance, healthcare, e-commerce, and social media.

However, this expansion has been accompanied by a corresponding rise in cybersecurity incidents and data breaches. Reports indicate a substantial increase in cyberattacks targeting Indian organizations, including ransomware attacks, phishing campaigns, and data leaks.[32] These incidents highlight the vulnerability of digital systems and raise concerns about the ability of organizations to implement effective data protection measures.

Another significant trend is the uneven level of compliance across sectors. Large corporations, particularly in the technology and financial sectors, have begun adopting structured data protection practices, often influenced by global standards. In contrast, smaller enterprises and informal sector entities continue to face difficulties in implementing compliance measures due to limited resources and awareness.

Further, empirical studies suggest that user awareness of data protection rights remains low. Many users are unaware of how their personal data is used or the rights available to them under the law.[33] This lack of awareness reduces the effectiveness of mechanisms such as consent and grievance redressal.

[31] Telecom Regulatory Authority of India (TRAI), The Indian Telecom Services Performance Indicators Report 2024–2025.
[32] Indian Computer Emergency Response Team (CERT-In), Annual Report 2025.
[33] Internet and Mobile Association of India (IAMAI), Consumer Privacy Survey Report 2024.

The emergence of data-driven business models has also intensified concerns regarding privacy. Companies increasingly rely on data analytics, targeted advertising, and behavioural profiling, often processing large volumes of personal data. While such practices contribute to economic growth, they also create risks of misuse and unauthorized access.

Another important trend is the growing reliance on digital public infrastructure, including platforms for payments, identity verification, and service delivery. While these systems enhance efficiency and accessibility, they also centralise large volumes of personal data, increasing the potential impact of data breaches.

In addition, the evolving nature of regulatory enforcement is evident in the gradual development of compliance practices. Organizations are in the process of adapting to new requirements, and regulatory authorities are still establishing enforcement mechanisms and interpretational guidelines.

Recent policy discussions have emphasised the need for strengthening cyber resilience, institutional capacity, and data governance frameworks to address these challenges.[34] However, the implementation of such measures remains ongoing.

Taken together, these trends indicate that while India has established a formal data protection framework, the ground reality reflects a system in transition, where compliance is uneven, enforcement is evolving, and risks continue to grow alongside digital expansion.

Critical Analysis

The preceding sections demonstrate that while the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 establish a structured compliance framework, their effectiveness in practice remains limited. A critical examination of the framework reveals a deeper issue namely, the misalignment between regulatory design and ground-level realities.

At the conceptual level, the framework reflects a compliance-oriented approach, where the emphasis is placed on fulfilling procedural requirements such as obtaining consent, issuing notices, and maintaining documentation. While these measures are essential for accountability, they do not necessarily ensure substantive protection of personal data. Compliance, in this sense, risks becoming a formal exercise rather than a meaningful safeguard.

[34] NITI Aayog, Data Governance and Cybersecurity Policy Updates (2025).

A central concern is the heavy reliance on consent as the primary basis for data processing. As discussed earlier, user behaviour is characterised by consent fatigue, lack of awareness, and unequal bargaining power. This creates a disconnect between the legal assumption of informed consent and the practical reality of passive user acceptance. Scholars have argued that consent-based models, when applied in complex digital environments, often fail to achieve genuine user autonomy.[35]

Further, the framework does not adequately incorporate a harm-based or outcome-oriented approach. The focus remains on whether procedural requirements have been followed, rather than on whether individuals have actually suffered harm due to data misuse. This limits the ability of the law to address emerging risks such as profiling, behavioural manipulation, and algorithmic bias.

Another critical issue is the over-reliance on regulatory discretion. The presence of broad and undefined terms, combined with evolving rules, creates a system where much depends on interpretation by authorities. This undermines legal certainty and increases the risk of inconsistent enforcement. Effective regulatory systems require clear standards and predictable outcomes, which are currently lacking in the Indian framework.

The analysis also reveals a structural tension between data protection and economic objectives. The simplified and flexible design of the DPDP framework appears to be aimed at facilitating ease of doing business and promoting digital growth. However, this approach may come at the cost of weaker privacy protections. Comparative studies have shown that robust data protection regimes often require stricter obligations and stronger enforcement mechanisms.[36]

Additionally, the gap between legal expectations and technological capacity presents a fundamental challenge. The framework assumes that organizations possess the infrastructure, expertise, and resources necessary to implement compliance measures. In reality, many entities lack such capacity, leading to uneven implementation and potential non-compliance.

Institutional limitations further exacerbate these issues. The enforcement mechanism, while formally established, is still evolving in terms of capacity, expertise, and procedural clarity. Without strong and independent regulatory institutions, even well-designed legal frameworks

[35] Neil M. Richards & Woodrow Hartzog, "The Pathologies of Digital Consent" (2019) 96 Washington University Law Review 1461.
[36] Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press, 2020).

may fail to achieve their objectives.

From a broader perspective, the Indian data protection regime reflects a transitional phase, where the law has been enacted but the ecosystem required for its effective functioning is still developing. This includes:

- regulatory capacity
- technological infrastructure
- user awareness
- industry preparedness

Thus, the key challenge lies not in the absence of law, but in the incomplete alignment between law, institutions, technology, and society.

In conclusion, the DPDP Act and Rules represent an important step forward, but their current design and implementation reflect a system that is procedurally robust yet substantively limited. Addressing this imbalance is essential for ensuring that data protection in India moves beyond formal compliance towards effective and meaningful privacy protection.

Conclusion

The introduction of the Digital Personal Data Protection Act, 2023 and the subsequent formulation of the Digital Personal Data Protection Rules, 2025 represent a significant step in India's effort to establish a structured and comprehensive data protection regime. Together, they mark a transition from a fragmented legal framework to a more coherent system of data governance.

However, as this paper demonstrates, the effectiveness of this framework cannot be assessed solely on the basis of its legislative design. The ground reality reveals a persistent gap between regulatory intent and practical implementation, shaped by a combination of legal, institutional, technological, and behavioural factors.

The compliance framework under the DPDP Rules, while detailed and structured, imposes substantial obligations on organizations that are not uniformly equipped to meet them. Financial constraints, lack of technical expertise, and infrastructural limitations hinder effective compliance, particularly among small and medium enterprises. At the same time, rapid technological advancements and increasing cyber threats further complicate the

implementation of data protection measures.

Equally significant is the role of user behaviour in shaping the effectiveness of the regime. The prevalence of consent fatigue, low levels of digital literacy, and asymmetry in bargaining power undermine the assumption that consent can function as a reliable mechanism for protecting privacy. This highlights the limitations of a consent-centric approach in the contemporary digital environment.

The analysis also reveals that the enforcement architecture, while formally established, is still evolving in terms of capacity, clarity, and consistency. Institutional limitations and regulatory ambiguity contribute to uncertainty in compliance and reduce the overall effectiveness of the framework.

Taken together, these factors indicate that India's data protection regime is currently in a transitional phase, where the legal framework exists but the ecosystem required for its effective functioning is still developing. The challenge, therefore, lies not merely in enacting laws, but in ensuring that they are supported by strong institutions, technological capacity, and informed user participation.

This paper argues that the current framework reflects a compliance-oriented model, which emphasises procedural adherence over substantive outcomes. While this approach facilitates regulatory implementation and economic flexibility, it may not fully achieve the objective of meaningful privacy protection.

In conclusion, the DPDP Act, 2023 and the DPDP Rules, 2025 provide a necessary foundation for data protection in India, but their success depends on bridging the gap between law and practice. This requires continuous regulatory refinement, institutional strengthening, and a shift towards a more holistic and outcome-oriented approach to data protection.