Critical study of Digital Personal Data Protection Rules 2025

Muktha T.V
Karnataka State Law University

Abstract—**The Digital Personal Data Protection Act, 2023 (DPDP Act) marks the first comprehensive legislation of India governing the processing of digital personal data and represents a major constitutional and regulatory response to the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India.[1] The notification of the Digital Personal Data Protection Rules, 2025 (DPDP Rules) operationalises the statutory framework by prescribing detailed obligations relating to notice and consent architecture, breach reporting, children's data protection, cross-border transfers, grievance redressal, and institutional governance. The Rules introduce a phased compliance structure, establish obligations for Significant Data Fiduciaries, and create a framework for Consent Managers, thereby reshaping India's digital governance landscape. This article critically evaluates the DPDP Rules, 2025 through constitutional, comparative, and regulatory lenses. It examines the extent to which the Rules strengthen informational privacy while simultaneously analysing concerns relating to executive overreach, institutional independence, state surveillance, cross-border data governance, and the dilution of transparency protections under the Right to Information Act, 2005. The article further compares the Indian framework with the European Union's General Data Protection Regulation (GDPR), particularly in relation to security safeguards, proportionality, and regulatory accountability. The article argues that while the DPDP Rules, 2025 constitute a transformative step toward establishing a consent-centric and accountability-driven privacy regime, the framework remains constrained by broad governmental exemptions, limited data principal rights, and excessive executive control over enforcement structures. The long-term legitimacy of India's data protection regime will therefore depend upon judicial interpretation, institutional independence, and the development of a balanced framework capable of reconciling privacy, innovation, transparency, and national security within a constitutional democracy.**

Index Terms—**DPDP Rules 2025, Data Protection Board, Consent Manager, Data Fiduciary, Informational Privacy, GDPR, Digital Constitutionalism**

I. INTRODUCTION

The legal genesis of data protection in India was decisively articulated in the landmark judgement of the Hon'ble Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India[2]. A nine-judge bench unanimously declared that the Right to Privacy is a fundamental right guaranteed under Article 21 and Part III of the Constitution[3]. The Court held that informational privacy is an essential facet of human dignity and autonomy, creating a constitutional imperative for the State to enact a comprehensive law to regulate personal data processing by both government and private entities. The Puttaswamy case laid the foundation for the evolution of Digital Personal Data Protection Act, 2023 (DPDP Act).

The legislative trajectory of the DPDP Act was significantly shaped by the J., B.N. Srikrishna Committee, which was constituted in 2017 to draft a data protection framework that balanced individual autonomy with the needs of the rapidly expanding digital economy. The Committee's 2018 report, titled A Free and Fair Digital Economy, introduced the foundational concept of the data fiduciary, arguing that the relationship between an individual and a

[1] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, (2017) 10 SCC 1, at p. 350

[2] Ibid, Supra note 1, at p.360

[3] Article 21 - Protection of Life and Personal Liberty: No person shall be deprived of his life or personal liberty except according to procedure established by law.

service provider is one based on trust.[4] This report served as the blueprint for several iterations of the law, including the Personal Data Protection Bills of 2019 and 2021. However, the 2023 Act ultimately streamlined the Committee's more prescriptive recommendations, such as the granular categorization of sensitive and critical personal data, in favour of a more simplified, technology-neutral approach.[5] By moving away from the complex sub-classifications found in earlier drafts, the current DPDP Act focuses on a singular definition of personal data, thereby reducing the clerical compliance burden while maintaining the core principal-fiduciary model first envisioned by the Srikrishna Committee.[6] The Act replaces the traditional Controller-Processor terminology with a more accountability-focused principal-fiduciary relationship. By using the term fiduciary, the law implies a higher duty of care and trust, suggesting that companies must act in the best interest of the user rather than treating data as a mere commodity. The Act moves toward a strictly consent-based regime. Consent must be affirmative and not a mere pre-ticked box. The doctrine of purpose limitation serves as a statutory barrier against the secondary processing of data, strictly confining its utilization to the specific objectives articulated in the initial notice. Companies must provide a notice detailing exactly what is being collected and the user's right to withdraw or complain. To prevent the framework from becoming a toothless tiger, the Act institutionalizes a robust enforcement regime designed to translate statutory principles into mandatory corporate accountability. The Act establishes the Data Protection Board of India (DPB) as its central enforcement pillar. Operating as a "digital-first," specialized adjudicatory body rather than a traditional civil court, the DPB is designed for procedural agility in the face of rapid technological shifts. Its primary mandate involves conducting inquiries into personal data breaches, resolving grievances initiated by Data Principals, and exercising its power to impose substantial financial penalties, reaching up to ₹250 Crores per contravention, to serve as a robust deterrent against corporate non-compliance. The Act is strictly limited to Digital Personal Data. This includes data collected online or data collected offline that is subsequently digitized. By narrowing the focus to digital ecosystems, the Act addresses the specific risks of the modern digital economy while providing a clearer compliance roadmap for global organizations operating across Indian jurisdictions.

To operationalize these statutory principles, the DPDP Rules, 2025 were notified on November 13, 2025, functioning as the critical bridge between the Act's normative framework and its practical implementation.[7] The Rules are framed in accordance with the SARAL (Simple, Accessible, Rational, and Actionable) philosophy. They delineate the procedural architecture necessary for compliance.[8] In doing so, they establish constitutional guarantees within the digital ecosystem by mandating itemized notices in regional languages and prescribing a stringent hour timeline for breach notifications, thereby rendering the right to informational privacy both scalable and enforceable.[9]

II. SALIENT FEATURES OF THE DPDP RULES, 2025

The DPDP Rules introduce a staggered 18-month implementation timeline focusing on consent management, breach notification, and children's data protection, with immediate, 1-year, and 18-month phased enforcement. Rules 1, 2 and 17 to 21 shall come into force on the date of their publication in the

[4] Committee. of experts under the Chairmanship of J., B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) [hereinafter Sri Krishna Report]

[5] *See* Personal Data Protection Bill, No. 373 of 2019; *see also* Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019 (2021).

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

[7] Digital Personal Data Protection Rules, 2025, Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025) https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf, last visited on March 05, 2026

[8] Ministry of Electronics and Information Technology, *Explanatory Note on the Digital Personal Data Protection Rules, 2025* (2025), https://www.meity.gov.in, last visited on January 20, 2026

[9] Digital Personal Data Protection Rules, at R. 7 prescribing rules for intimation of personal data breach and timeline).

Official Gazette. Rule 4 shall come into force one year after the date of publication of this Gazette. Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of Official Gazette.[10]

A. Notice and Consent Framework

Rule 3 and 4 of the DPDP Rules operationalize a detailed notice and consent framework requiring data fiduciaries to provide clear, itemized notices specifying purpose, categories of personal data, retention periods, and grievance mechanisms.[11] The Rules mandate that consent must be free, specific, informed, and unambiguous, and must be capable of withdrawal with ease. This reflects a shift from formal compliance to substantive transparency.[12] A distinctive feature of Rule 4 is the introduction of consent Managers' registered entities that enable data principals to manage consent across platforms. Consent Managers occupy a central position within the data protection architecture, serving as essential intermediaries that empower Data Principals to maintain autonomy over their personal information. Rule 4 delineates the mandatory registration protocols, fiduciary duties, and comprehensive compliance standards governing these entities. These intermediaries are subject to obligations of neutrality, security, and accountability, reflecting a move toward user-centric data governance architectures. Rule 5 deals with the regulatory framework concerning the state's processing of personal data for the distribution of subsidies, licenses, and public services is fundamental to balancing administrative efficiency with the statutory protections afforded to individuals under the DPDP Act.

B. Security Safeguards and Breach Notification

Rule 6 prescribes specific technical and organizational measures, including encryption, access controls, logging, and periodic audits. At its core, reasonable security safeguards refer to a comprehensive framework that protects personal data from breaches and unauthorized access. This marks a transition from broad statutory obligations to granular compliance requirements, aligning with global cybersecurity norms. This responsibility extends beyond the Data Fiduciary to include any Data Processor acting on its behalf. The rule outlines specific measures that set the minimum threshold for data protection practices. Rule 7 of the DPDP Act mandates robust protocols for notifying affected parties and the Board, ensuring transparency, accountability, and a swift response to mitigate risks. Rule 8 of the DPDPA underscores the importance of purposeful data retention. By defining clear timelines for data erasure and mandating proactive notifications, it strikes a balance between organizational needs and individual privacy. For Data Fiduciaries, compliance is not just about meeting legal requirements, it is about fostering trust and demonstrating respect for the data entrusted to them. This rule sets a new benchmark for responsible data management, ensuring that personal data serves its purpose without overstaying its welcome in the digital ecosystem. It emphasises timely and clear communication in the event of a personal data breach. When a data breach occurs, the data fiduciary is obligated to notify both the affected data principals and the board for the affected individual to take proactive steps to safeguard their interests, and in case of the regulatory authorities the notification shall pave way to assess the broader implications. The rule outlines specific triggers and timelines for data erasure. It mandates that personal data be erased when a data principal has neither engaged with the data fiduciary toward the original purpose nor exercised their statutory rights within the timeframe specified in Schedule III, provided no legal retention

[10] Rule 1 establishes the commencement date of the rules through a multi-stage activation, where foundational mandates become enforceable immediately, whereas complex provisions such as consent mechanisms, individual rights, and protections for minors are granted a deferred timeline. Rule 2 defines key terms used across the rules, complementing the definitions in the DPDP Act 2023. Rule 17 focuses on the constitution and appointments of the Data Protection Board. Rule 18 outlines the salary, allowances, and service terms for the Chairperson and members. Rule 19 sets procedures for Board meetings and authentication of orders. Rule 20 establishes the Board's functioning as a digital office, allowing for virtual operations. Rule 21 defines terms and conditions of appointment for Board officers and employees.

[11] Digital Personal Data Protection Rules, 2025, Gazette of India (Nov. 13, 2025) Rule 3 - Rule 3 DPDP Rules 2025 - Notice given by Data Fiduciary to Data Principal.

[12] Ibid, Supra note 10, at 4

requirements apply. To prevent unintended data loss, the data fiduciary must issue notification atleast 48 hours prior to such erasure, serving as a final opportunity for the data principals to re-engage, access their account, or exercise their rights to correct or object to processing. This dual-layered mechanism harmonizes corporate accountability with individual autonomy, ensuring that the data lifecycle remains transparent and that data principals retain active control over their personal information. Rule 9 deals with Rule 9 accessibility and clarity. Rule 9 prioritizes accessibility and transparency by mandating the prominent disclosure of contact information of the Data Protection Officer (DPO) or an authorized representative across all digital platforms. This requirement extends to formal correspondence, ensuring that every response to a data principal's request includes direct contact details to facilitate seamless follow-up and continuity. The designated representative must possess the authority and technical knowledge to provide substantive, accurate responses regarding the organization's processing activities. By formalizing these communication channels, Rule 9 ensures that the right to information is supported by an accountable and responsive corporate structure. By aligning with international benchmarks like the GDPR, Rule 9 underscores a commitment to transparency and seamless accessibility through clearly defined contact points. This specific provision significantly enhances India's stature within the international privacy domain while reckoning a robust regulatory shift. The adoption of such measures under the DPDP Rules, 2025, demonstrates that the national framework is both exhaustive and deeply rooted in the principles of user autonomy. The legislative provision of section 9(1) of the DPDP Act mandates that data fiduciaries must, before processing any personal data of a child or person with disability, obtain verifiable consent from the parent or lawful guardian of such child or person with disability. Further section 9(3) prohibits processing of personal data that is likely to cause harm to the child.

C. Children's Data and Persons with Disabilities

Rule 10 of the DPDP Rules provides an exemption to the aforementioned legal mandates under section 9(1) and section 9(3) of the DPDP Act. Rule 10 provides that provisions of sub-sections (1) and (3) of section 9 shall NOT be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to conditions specified therein. In other words, the Rule 10 exempts only to sub-sections (1) and (3) of section 9. The other obligations such as General obligations of Data Fiduciaries under section 8, consent requirements under section 6, any provisions specifically exempted under section 9(2), Data breach notifications, grievance redressal, and as such remain applicable even when exemption applies under Rule 10. Rule 11 provides a protective as well as a complex regulatory framework designed to safeguard the personal data of persons with disabilities who have lawful guardians. Part B of Fourth Schedule is yet to be implemented. Rule 11 makes it mandatory that consent obtained from the legal guardian is verified before processing the data of persons with disabilities, dual verification of the legal guardian's identity and adulthood, implementation of reasonable technical and organizational security measures, high penalties on Data Fiduciaries in case of breach and balances the autonomy and the protection of persons with disabilities. Under Rule 12, certain Data Fiduciaries can bypass specific obligations found in section 9 of the DPDP Act regarding children's data (individuals under 18). These exemptions are not absolute; they only apply to specific categories of fiduciaries or purposes outlined in the Fourth Schedule and are contingent upon meeting rigorous safety standards, documentation, and protective safeguards. The Fourth Schedule facilitates these exemptions through two primary frameworks: entity-based and purpose-based criteria. Under Part A, specific organizations such as healthcare providers, educational institutions, and child-care or transport services are granted limited relief from stringent verifiable-consent requirements, recognizing their essential role in a child's development and well-being. Complementing this, Part B outlines purpose-based exemptions that allow for the processing of the data of a minor without standard consent formalities in critical scenarios, including emergency medical interventions, safety monitoring, statutory legal compliance, or specialized research and archival tasks. In both instances, these exemptions are not absolute but remain strictly contingent upon the data fiduciary's adherence to predefined safety conditions and rigorous data protection safeguards. Non-

compliance of this rule by the data fiduciaries shall result into enforcement, fines, and reputational damage.

D. Significant Data Fiduciaries

Rule 13 of the DPDP Rules 2025 imposes a heightened compliance burden for entities designated as Significant Data Fiduciaries (SDFs) under section 10 of the DPDP Act, 2023, reflecting their profound influence over the digital ecosystem and the potential risks their processing activities pose to Data Principals. By mandating annual Data Protection Impact Assessments (DPIAs) and independent audits, the rule shifts the regulatory focus from mere self-reporting to structured, transparent accountability, requiring that significant observations be shared directly with the Board. Significant observations are not defined under the Rules. The definition shall be extrapolated based on Material compliance gaps or violations, High-risk processing activities, Systemic weaknesses in data protection framework, and remediation plan. Furthermore, the rule introduces a proactive duty of care regarding algorithmic transparency and technical due diligence to pre-emptively mitigate systemic risks to individual rights. Rule 13 (4) reinforces digital sovereignty of India by empowering the Central Government to impose data localization requirements on specific categories of personal and traffic data, ensuring that sensitive information remains within domestic jurisdiction under the oversight of a specialized inter-ministerial committee. Breach of SDF obligations under section 10 attracts penalty up to ₹150 crore. Additionally, if the breach invokes Data Localization obligations, Blocking orders shall be passed under section 37 (Government power to block access) of the DPDP Act. Further, Rule 1(4) specifies that Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of this Gazette. DPDP Act is the first Indian law in the world to explicitly mandate due diligence on Artificial Intelligence and Machine Learning systems of the significant data fiduciaries processing personal data.

E. Rights of Data Principals

The DPDP Act recognises several statutory rights designed to strengthen informational autonomy and ensure greater accountability in the processing of personal data. These rights collectively reflect the Act's attempt to establish a consent-centric privacy framework while balancing individual interests with legitimate data processing requirements. The rights of Data Principals are primarily enumerated under Sections 11 to 14 of the DPDP Act and are operationalised through Rule 14 of the DPDP Rules, 2025.

Section 11 of the DPDP Act grants the Data Principal the right to access information regarding the processing of personal data. This includes the right to obtain a summary of the personal data being processed, the identities of Data Fiduciaries and Data Processors with whom such data has been shared, and a description of the processing activities undertaken. This provision enhances transparency by enabling individuals to understand how their personal data is collected, stored, used, and disseminated within digital ecosystems.

Section 12 provides the right to correction, completion, updating, and erasure of personal data. Data Principals may require Data Fiduciaries to correct inaccurate or misleading data, complete incomplete information, update outdated personal data, or erase data that is no longer necessary for the purpose for which it was collected, subject to legal retention obligations. This right reflects the broader principle of data accuracy and purpose limitation embedded within modern privacy jurisprudence.

Section 13 recognises the right to grievance redressal. Under this provision, Data Principals may seek redress against acts or omissions of Data Fiduciaries or Consent Managers relating to the processing of personal data. If unsatisfied with the response provided by the Data Fiduciary, the Data Principal may escalate the grievance before the Data Protection Board of India. The grievance redressal mechanism is intended to strengthen procedural accountability and provide an accessible remedy framework within the data protection regime.

Section 14 introduces the right to nominate, which enables a Data Principal to nominate another individual who may exercise the rights of the Data Principal in the event of death or incapacity. This provision constitutes a distinctive feature of the Indian data protection framework and reflects legislative recognition of digital succession and informational continuity. The provision is particularly significant for elderly persons, minors, or individuals suffering from incapacity.

Rule 14 of the DPDP Rules, 2025 operationalises these statutory rights by prescribing procedural obligations for Data Fiduciaries and Consent Managers. Rule 14 requires Data Fiduciaries to publish the manner through which Data Principals may exercise their statutory rights and mandates the implementation of appropriate technical and organisational measures to ensure timely compliance with such requests. Rule 14(3) specifically obligates Data Fiduciaries and Consent Managers to publicly disclose the timelines within which grievances and requests shall be addressed. This enhances transparency and ensures greater predictability within the grievance redressal process. In other words, in addition to transparency, Rule 14 it also mandates accountability. Rule 14 also touches upon a unique right, the right to nominate. Under Rule 14(4), a Data Principal can nominate individuals to exercise their rights on their behalf. This provision is particularly helpful for scenarios involving incapacitated individuals or minors or elderly persons.

The rights framework under the DPDP Act reflects India's evolving commitment toward informational self-determination and digital accountability. However, unlike the European Union's General Data Protection Regulation (GDPR), the Indian framework does not expressly recognise certain important rights such as data portability and a fully articulated right to be forgotten. Consequently, although the DPDP framework strengthens procedural safeguards, critics argue that it remains comparatively limited in its recognition of substantive privacy rights available under mature international data protection regimes.

F. Cross-Border Data Transfers

Rule 15 deals with any personal data transferred outside the territory of India. Rule 15 of the DPDP Rules, 2025 gives effect to section 16 of the DPDP Act. Rule 15 establishes a permissive default.[13] In other words, the personal data of individuals data processed by a Data Fiduciary may be transferred outside India. There is no blanket prohibition. The transfer is permitted unless the Central Government, through an order, imposes specific restrictions. Unlike the European Union's GDPR, which relies on a detailed adequacy-decision framework, bilateral agreements, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs), India's approach under Rule 15 is characterised by deliberate executive flexibility. Rule 15 provides that the Data Fiduciary may transfer the personal data outside of India subject to meeting such requirements as specified by the Central Government through a general or a special order. Such requirements include Country level restrictions, Data category restrictions, Contractual safeguards, Technical safeguards, Reporting obligations. Country level restrictions refer to the list of countries to which transfers are prohibited or restricted in alignment with EU's "non-adequate" country list under GDPR Article 45. Data category restrictions relate to special requirements for sensitive categories of data such as financial data, health data, children's data. Contractual safeguards mandate specific clauses in data transfer agreements like Standard Contractual Clauses in the EU. Technical safeguards prescribe the encryption standards, anonymisation requirements, or data residency requirements for mirror copies. Reporting obligations provide for the disclosures to the Data Protection Board about cross-border flow. Rule 15 specifically restricts transfers to any foreign State, Any person or entity under the control of a foreign State, Any agency of such a State. In other words, if the Central Government restricts transfer to a country A, then the transfer to country A between 2 corporates in a private sector is prohibited albeit they are governed by a private contract. Further Rule 15 works in tandem with sector specific compliance and does not over-ride it. In cases of overlap, stricter norms prevail. Rule 16 provides for exemption to processing of personal data for the purposes of research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.

G. Institutional Governance and Adjudication

Rule 17 provides for the appointment of chairperson and other members. Cabinet secretary shall be the chairperson. The Rules establish two distinct committee structures based on the seniority of the role being filled. In case of the appointment of the chairperson, the committee is led by the cabinet secretary. It includes the secretaries of the Department of Legal Affairs and the Ministry of Electronics and Information Technology (MeitY),

[13] https://www.dpdpa.com/dpdparules/rule15.html, last visited on May 05, 2026

along with two government-nominated experts. For the appointment of other members, the committee is led by the Secretary of MeitY. It maintains a similar structure with the Secretary of Legal Affairs and two external experts. While the Committees recommend candidates based on "special knowledge or practical experience," the final power of appointment rests solely with the Central Government. The government is required to "consider the suitability" of the recommended individuals before making the formal appointment. Furthermore, sub-rule (4) provides a legal shield, ensuring that the committee's proceedings cannot be challenged or invalidated simply because of a vacancy or a technical defect in how the committee was formed. Rule 18 provides for the Salary, allowances and other terms and conditions of service of Chairperson and other Members, as specified in Fifth Schedule. Rule 19 prescribes Procedure for meetings of Board and authentication of its orders, directions and instruments. Rule 20 provides that the Board shall function as a "Digital Office". It denotes a paradigm shift from traditional, in-person hearings to a predominantly virtual setup, thereby realising India's Digital initiative. This move sets a precedent for other regulatory bodies, highlighting the advantages of digital transformation in public administration. Rule 21 sets the terms and conditions of appointment and service of officers and employees of Board as are specified in Sixth Schedule. Rule 22 prescribes the procedure to file an appeal by a person aggrieved by the order or direction of the Board. It explicitly states that the appeal shall be filed digitally and the Tribunal is not governed by the code of Civil procedure but by the principles of natural justice. The tribunal is empowered to form its own rules and procedures to hear the appeal, thereby fast-tracking the proceedings without having to go through the adversarial procedure. Rule 23 states that the central government may call the data fiduciary or the intermediary to furnish such information as may be called for provided that such information does not affect the sovereignty and integrity of India or the security of the state. In such instances the information may only be shared with the affected data principal after obtaining prior permission from the central government in writing. For the purposes of this rule, the expression "intermediary" shall have the same meaning as assigned to it in the Information Technology Act, 2000 (21 of 2000).

III. REGULATORY SCHEDULES UNDER THE DPDP RULES, 2025

Schedule I of the DPDP Rules prescribes the conditions for the registration of Consent Managers and outlines the obligations imposed upon Consent Managers under the Act.

Schedule II prescribes the standards for the processing of personal data by the State and its instrumentalities under clause (b) of Section 7, as well as for the processing of personal data necessary for the purposes specified under clause (b) of sub-section (2) of Section 17 of the DPDP Act.

Schedule III provides a table specifying the classes of Data Fiduciaries, the purposes of data processing, and the corresponding time periods for the erasure of the personal data of a Data Principal. The relevant period is calculated from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose, exercised her rights, or from the commencement of the DPDP Rules, 2025, whichever is later. A Data Fiduciary belonging to such class and processing personal data for such corresponding purposes as specified in Schedule III shall erase such personal data, unless its retention is necessary for compliance with any law for the time being in force, if the Data Principal neither approaches the Data Fiduciary for the specified purpose nor exercises her rights in relation to such processing within the prescribed time period.

Schedule IV provides a table of classes of Data Fiduciaries, including clinical establishments, healthcare establishments, healthcare professionals, educational institutions, crèches, and child-care providers, in respect of whom the provisions of sub-sections (1) and (3) of Section 9 of the DPDP Act, read with Rule 11 of the DPDP Rules, shall not apply.

Schedule V prescribes the remuneration, benefits, and other terms and conditions of service of the Chairperson and other Members of the Search and Selection Committee constituted under Rule 17.

Schedule VI provides for the appointment of officers and employees of the Board and specifies their entitlements, including gratuity, travelling allowances, medical assistance, leave, and other terms and conditions of service.

Schedule VII specifies the purposes for which Data Fiduciaries or intermediaries may be required, under Rule 22 of the DPDP Rules, to furnish personal information of a Data Principal to the State or its instrumentalities in the interests of the sovereignty and integrity of India or the security of the State. The Schedule also identifies the authorised persons permitted to use such personal data for the purposes specified therein.

IV. CRITICAL ANALYSIS OF THE DPDP RULES

The DPDP Rules procedural clarity regarding notice requirements, consent management, breach reporting, data retention, children's data protection, and cross-border transfers. In doing so, they represent a notable advancement over the fragmented regime that previously existed under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Nevertheless, despite their transformative potential, the DPDP Rules have generated substantial criticism concerning executive overreach, regulatory ambiguity, weak institutional independence, and insufficient safeguards against state surveillance.

Small and Small and Medium Enterprises (SMEs) may face challenges in implementing the advanced security measures and consent frameworks required under the DPDP Rules. The obligation to notify the DPB and affected individuals for all breaches could overwhelm regulatory systems and reduce focus on critical incidents. Certain aspects, such as the role and accountability of Consent Managers, require further clarification to avoid gaps in implementation. The stringent requirements for processing children's data could create logistical hurdles for Data Fiduciaries.

A significant strength of the Rules lies in their attempt to operationalise informed consent through itemised notices, multilingual accessibility, and mechanisms for withdrawal of consent. The framework also introduces "Consent Managers," thereby institutionalising intermediary based consent governance in a manner loosely comparable to the European Union's General Data Protection Regulation (GDPR). These provisions reflect an effort to enhance informational self-determination and user autonomy in digital ecosystems. However, critics argue that the Rules remain excessively dependent on formalistic consent models that fail to account for structural inequalities between users and large technology platforms. In practice, individuals frequently lack the time, expertise, or bargaining power necessary to meaningfully evaluate privacy notices, resulting in what scholars describe as "consent fatigue."[14] Consequently, the consent architecture risks devolving into a procedural compliance exercise rather than a substantive mechanism for protecting privacy rights. This undermines the normative goal of informational self-determination.[15] Certain provisions remain vague, leading to uncertainty in implementation and potential regulatory inconsistencies.[16]

The Rules also impose cybersecurity and breach notification obligations upon Data Fiduciaries by requiring reasonable security safeguards, access controls, logging mechanisms, and reporting obligations. These provisions indicate an attempt to align India's data governance framework with international standards, particularly Article 32 of the GDPR. However, the DPDP Rules provide limited technical specificity regarding encryption thresholds, anonymisation standards, or measurable cybersecurity benchmarks. The absence of a clearly articulated risk based framework creates interpretive uncertainty for businesses and may lead either to excessive compliance expenditure or superficial compliance practices designed merely to avoid regulatory penalties.[17] Unlike the GDPR, which incorporates a nuanced proportionality-based compliance structure, the DPDP Rules adopt a comparatively broad and discretionary approach that leaves critical operational questions unresolved.

Another important feature of the DPDP Rules concerns cross-border data transfers. Earlier iterations of India's data protection proposals, particularly the Personal Data Protection Bill, 2019, contemplated extensive localisation obligations. The DPDP Rules adopt a comparatively liberal approach

[14] Solove, Daniel J., *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013)
[15] Ibid, Supra note 14 at 11
[16] See Internet Freedom Foundation, *Analysis of DPDP Rules* (2025)
[17] Graham Greenleaf, *India's DPDP Rules and the Future of Privacy Compliance*, 182 Privacy Laws & Bus. Int'l Rep. 1 (2025).

by permitting overseas transfers except to jurisdictions specifically restricted by the Central Government. This model supports India's aspirations as a global digital economy and preserves operational flexibility for multinational corporations, outsourcing entities, and cloud service providers. However, the framework simultaneously vests substantial discretionary authority in the executive regarding restricted jurisdictions and transfer conditions. Unlike the GDPR adequacy regime, the DPDP Rules do not establish transparent criteria, independent oversight, or procedural review mechanisms governing such decisions.[18] This regulatory uncertainty may undermine business predictability and complicate India's aspirations for global interoperability in digital trade and data governance.

The most sustained criticism of the DPDP Rules concerns the concentration of regulatory power within the executive branch. The Central Government exercises extensive authority over the constitution, functioning, and administration of the Data Protection Board of India, as well as the classification of Significant Data Fiduciaries (SDF) and the scope of exemptions under the Act. This institutional design has generated concerns regarding the independence and impartiality of the enforcement mechanism, particularly because the State itself is one of the largest processors of personal data.[19] Unlike independent supervisory authorities under the GDPR, the Indian framework lacks sufficient structural insulation from executive influence. Such concentration of power raises constitutional concerns relating to separation of powers, procedural fairness, and accountability, especially in light of the proportionality doctrine articulated in Justice K. S. Puttaswamy (Retd.) v. Union of India.[20]

Equally controversial are the broad exemptions available to State agencies on grounds such as sovereignty, public order, national security, and prevention of offences. The Rules fail to prescribe robust procedural safeguards, independent authorisation requirements, or effective oversight mechanisms governing state access to personal data. In the context of India's expanding digital governance infrastructure, including Aadhaar-linked databases, facial recognition technologies, and integrated public digital platforms, these exemptions have intensified concerns regarding mass surveillance and informational asymmetry between citizens and the State.[21] The absence of meaningful judicial or parliamentary oversight mechanisms distinguishes the Indian framework from several comparative jurisdictions where national security exemptions remain subject to proportionality review and independent scrutiny.

DPDP framework has additionally been criticised for its potential impact upon transparency and democratic accountability. Amendments associated with the privacy regime have been viewed as capable of diluting the effectiveness of the Right to Information Act, 2005 (RTI Act) by broadening exemptions relating to "personal information." Prior to the enactment of the DPDP framework, section 8(1)(j) of the RTI Act permitted the withholding of personal information only when disclosure had no relationship to public activity or would cause an unwarranted invasion of privacy, unless a larger public interest justified disclosure. The DPDP Act amended this provision by broadening the exemption relating to "personal information," thereby removing the earlier emphasis on public interest balancing. Critics argue that this amendment may allow public authorities to deny access to information concerning public officials, recruitment processes, public expenditure, disciplinary proceedings, and other matters involving governmental accountability merely on the ground that such information relates to identifiable individuals.[22] Indian constitutional jurisprudence, particularly Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal[23] and Puttaswamy[24], has consistently recognised that privacy and transparency are co-equal constitutional values requiring contextual balancing

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council art. 45, 2016 O.J. (L 119) 1 (EU)

[19] Apar Gupta & Mishi Choudhary, *India's Data Protection Framework and the Crisis of Regulatory Independence*, Internet Freedom Found. Working Paper (2025).

[20] Ibid, Supra note 1, at p.300

[21] Ibid

[22] Ibid, Supra note 2, at p.50

[23] *Central Public Information Officer, Supreme Court of India* v. *Subhash Chandra Agarwal*, (2020) 5 SCC 481

[24] Ibid, Supra note 1, at p. 350

rather than absolute prioritisation of one over the other.[25] Critics therefore contend that the amended framework risks creating a culture of secrecy inconsistent with democratic accountability, particularly in an era of expanding state surveillance and digital governance. The future judicial interpretation of these amendments will be crucial in determining whether India can preserve transparency while simultaneously protecting informational privacy. Journalists, civil society organisations, and transparency advocates have argued that such provisions may hinder investigative journalism and restrict public access to information concerning governmental functioning.[26] This tension between privacy and transparency highlights the broader constitutional challenge of balancing informational privacy with democratic accountability in an increasingly digitised state apparatus.

From an economic perspective, the compliance obligations introduced by the Rules may disproportionately affect small and medium enterprises ("SMEs"). Large technology corporations possess the institutional capacity to implement consent management systems, cybersecurity audits, grievance redressal frameworks, and vendor governance mechanisms. Smaller businesses, however, may struggle with the financial and technical burdens associated with compliance.[27] Consequently, the Rules may inadvertently reinforce market concentration by privileging large entities capable of absorbing regulatory costs while disadvantaging emerging startups and smaller enterprises. This concern is particularly relevant in the Indian context, where SMEs constitute a substantial component of the digital economy.

A key criticism of the DPDP framework is the breadth of exemptions available to the State.[28] These exemptions risk undermining the constitutional guarantee of privacy by enabling disproportionate state surveillance. The absence of explicit exemptions for journalistic activities raises concerns regarding the chilling effect on free speech and investigative journalism.[29] The detailed compliance requirements, particularly in relation to audits, logging, and consent management, impose significant operational costs, disproportionately affecting small and medium enterprises.[30] Unlike the EU General Data Protection Regulation (GDPR), the DPDP framework lacks key rights such as data portability and a fully articulated right to be forgotten. This results in a comparatively weaker rights based framework.[31] The Rules confer extensive powers on the Central Government, particularly in relation to exemptions and cross-border data transfers. This raises concerns regarding over-centralization and the absence of an independent regulatory authority.[32] A critical evaluation reveals that a major strength of the Rules is their move beyond abstract obligations toward operational security controls that encourage end to end data protection and integrate both technical and organizational safeguards. However, there are notable limitations, including a lack of precise technical benchmarks, such as specific encryption standards, and a heavy compliance burden that disproportionately affects small and medium enterprises (SMEs). Additionally, there is ambiguity regarding what constitutes reasonable safeguards and potential overlap with existing frameworks like the IT Act and CERT-In[33] guidelines.

V. CONCLUSION

The Digital Personal Data Protection Rules, 2025 represent a transformative development in India's evolving framework of digital constitutionalism and

[25] Ibid

[26] Internet Freedom Foundation, Comments on the Draft Digital Personal Data Protection Rules, 2025 (2025).

[27] NASSCOM, *Industry Concerns on DPDP Compliance Burdens for SMEs* (2025).

[28] Ibid Supra note 2, at p.65

[29] *Anuradha Bhasin* v. *Union of India*, (2020) 3 S.C.C. 637 (India)

[30] NASSCOM, Industry Feedback on DPDP Implementation (2025)

[31] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 20–21

[32] *Digital Personal Data Protection Act*, 2023, Sections 16–17.

[33] CERT-In (Indian Computer Emergency Response Team) guidelines, issued under the IT Act 2000, mandate strict cybersecurity practices, including reporting incidents within six hours. Key guidelines cover data security, identity management, and incident response, with specific mandates for government, MSMEs, and service providers (VPNs, Cloud).

informational privacy governance. The Rules signify a substantial departure from the fragmented regulatory framework that previously existed under the Information Technology Act, 2000 and the Information Technology Rules, 2011. In doing so, they strengthen procedural accountability and seek to harmonise India's data governance framework with emerging international standards, particularly the principles embodied in the European Union's General Data Protection Regulation (GDPR). By prescribing detailed obligations relating to notice architecture, consent management, breach reporting, data retention, children's data protection, and cross-border data transfers, the Rules operationalise the Digital Personal Data Protection Act, 2023. By introducing detailed compliance obligations, security safeguards, and enforcement mechanisms, they enhance procedural accountability. The Rules represent a landmark development in India's evolving digital constitutionalism and data governance architecture. The Rules undoubtedly provide long-awaited operational clarity and establish foundational compliance mechanisms that may strengthen digital trust and harmonise India's framework with emerging global standards. However, the framework remains constrained by, expansive state exemptions, limited data principal rights, and centralized regulatory control. For the DPDP regime to fully realize the constitutional promise of privacy, future reforms must focus on strengthening individual rights, ensuring regulatory independence, and clarifying compliance obligations. The ultimate legitimacy and effectiveness of the framework will therefore depend not merely upon statutory implementation but upon judicial interpretation, institutional accountability, and the extent to which privacy is treated as a substantive constitutional guarantee rather than an instrument of administrative governance.

REFERENCES

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at p. 350

[2] Ibid, Supra note 1, at p.360

[3] Article 21 - Protection of Life and Personal Liberty: No person shall be deprived of his life or personal liberty except according to procedure established by law.

[4] Committee. of experts under the Chairmanship of J., B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) [hereinafter Sri Krishna Report] See Personal Data Protection Bill, No. 373 of 2019; see also Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019 (2021).

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

[6] Digital Personal Data Protection Rules, 2025, Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025)

[7] https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf, last visited on March 05, 2026 Ministry of Electronics and Information Technology, Explanatory Note on the Digital Personal Data Protection Rules, 2025 (2025), https://www.meity.gov.in, last visited on January 20, 2026

[8] Digital Personal Data Protection Rules, at R. 7 prescribing rules for intimation of personal data breach and timeline).

[9] Rule 1 establishes the commencement date of the rules through a multi-stage activation, where foundational mandates become enforceable immediately, whereas complex provisions such as consent mechanisms, individual rights, and protections for minors are granted a deferred timeline. Rule 2 defines key terms used across the rules, complementing the definitions in the DPDP Act 2023. Rule 17 focuses on the constitution and appointments of the Data Protection Board. Rule 18 outlines the salary, allowances, and service terms for the Chairperson and members. Rule 19 sets procedures for Board meetings and authentication of orders. Rule 20 establishes the Board's functioning as a digital office, allowing for virtual operations. Rule 21 defines terms and conditions of appointment for Board officers and employees.

[10] Digital Personal Data Protection Rules, 2025, Gazette of India (Nov. 13, 2025) Rule 3 - Rule 3 DPDP Rules 2025 - Notice given by Data Fiduciary to Data Principal.

[11] Ibid, Supra note 10, at 4

[12] https://www.dpdpa.com/dpdparules/rule15.html, last visited on May 05, 2026

[13] Solove, Daniel J., Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013)

[14] Ibid, Supra note 14 at 11

[15] See Internet Freedom Foundation, Analysis of DPDP Rules (2025)

[16] Graham Greenleaf, India's DPDP Rules and the Future of Privacy Compliance, 182 Privacy Laws & Bus. Int'l Rep. 1 (2025).

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council art. 45, 2016 O.J. (L 119) 1 (EU)
[18] Apar Gupta & Mishi Choudhary, India's Data Protection Framework and the Crisis of Regulatory Independence, Internet Freedom Found. Working Paper (2025).
[19] Ibid, Supra note 1, at p.300
[20] Ibid
[21] Ibid, Supra note 2, at p.50
[22] Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481
[23] Ibid, Supra note 1, at p. 350
[24] Ibid
[25] Internet Freedom Foundation, Comments on the Draft Digital Personal Data Protection Rules, 2025 (2025).
[26] NASSCOM, Industry Concerns on DPDP Compliance Burdens for SMEs (2025).
[27] Ibid Supra note 2, at p.65
[28] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India)
[29] NASSCOM, Industry Feedback on DPDP Implementation (2025)
[30] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 20–21
[31] Digital Personal Data Protection Act, 2023, Sections 16–17.