INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER

AUTHOR – MS. AASHI DIXIT, BBA-LL.B (Hons.), LL.M. NET (LAW), INDEPENDENT ACADEMIC RESEARCHER

BEST CITATION - MS. AASHI DIXIT, DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (1) OF 2026, PG. 116-130, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI – https://doi.org/10.65393/LDEO6679

I. Abstract

The Digital Personal Data Protection Act, 2023 represents a landmark development in India's legal and regulatory framework governing the collection, processing, storage, and protection of personal data. Enacted in the aftermath of the Supreme Court's historic recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017), the Act responds to a long-standing constitutional and legislative vacuum in data protection. In an era marked by rapid digitalization, expanding State surveillance capabilities, and the growing economic significance of data-driven innovation, the DPDP Act seeks to establish a consent-based regulatory regime that balances individual privacy, national interests, and economic development. This paper undertakes a critical evaluation of the DPDP Act, 2023 to assess whether it adequately complies with the constitutional standards articulated in *Puttaswamy*, particularly the requirements of legality, necessity, proportionality, and procedural safeguards. It interrogates the extent to which the Act protects informational autonomy and individual dignity while permitting data processing by the State and private entities. Special attention is devoted to examining the breadth of State exemptions, which allow the government to process personal data for purposes such as national security, public order, and governance, raising concerns about unchecked executive discretion and the potential normalization of mass surveillance.The study further analyzes the Act's consent architecture, enforcement mechanisms, and institutional design, including the powers and independence of the Data Protection Board of India. It evaluates whether the absence of an independent, judicially insulated regulator and the limited avenues for redress weaken the effectiveness of data protection guarantees. Through a comparative analysis with global data protection frameworks, particularly the European Union's General Data Protection Regulation (GDPR), the paper highlights both areas of convergence-such as recognition of data principal rights-and significant divergences, especially regarding State accountability, regulatory independence, and proportionality constraints. The paper argues that while the DPDP Act, 2023 constitutes an important step toward formalizing data protection in India, it simultaneously consolidates significant power in the executive, thereby raising serious concerns about constitutional compliance, democratic accountability, and the dilution of privacy protections. It concludes that without stronger safeguards, clearer limitations on State power, and enhanced institutional independence, the Act risks prioritizing governance efficiency and economic interests over the fundamental right to privacy, necessitating urgent legal and structural reforms.

Keywords: Digital Personal Data Protection Act, 2023; Right to Privacy; State Surveillance; Data Governance; Constitutional Proportionality

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

II. Introduction

The exponential expansion of digital governance, surveillance infrastructures, and data-driven economic models has fundamentally altered the nature of personal data, transforming it into a strategic resource of immense value for both State authority and commercial enterprise. Governments increasingly rely on large-scale data collection to administer welfare schemes, enhance security, and deliver public services, while private corporations leverage personal data to drive innovation, targeted advertising, and algorithmic decision-making. In this context, personal data has emerged not merely as an informational asset but as a tool capable of shaping individual autonomy, social behavior, and power relations within democratic societies. In India, this transformation occurred in the absence of a comprehensive data protection regime for several decades. Despite the rapid digitization of governance through initiatives such as Aadhaar, Digital India, and platform-based public service delivery, regulatory oversight remained fragmented and sector-specific, governed by limited provisions under the Information Technology Act, 2000 and subordinate rules. This regulatory vacuum persisted even as the scale and sensitivity of personal data processing expanded dramatically, raising serious concerns regarding surveillance, profiling, data misuse, and the erosion of individual privacy. The lack of a coherent legal framework not only exposed citizens to privacy violations but also undermined public trust in digital governance mechanisms.

A decisive constitutional shift occurred with the Supreme Court's landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017), which unequivocally recognized the right to privacy as a fundamental right intrinsic to life and personal liberty under Article 21 of the Constitution. The Court articulated a principled framework requiring any infringement of privacy to satisfy the tests of legality, necessity, proportionality, and procedural safeguards. This judgment created a binding constitutional mandate for the State to enact a robust data protection law that would regulate both State and non-State actors while safeguarding informational autonomy and individual dignity. It is against this constitutional, technological, and regulatory backdrop that the Digital Personal Data Protection Act, 2023 was enacted.

The Act marks a significant transition in India's approach to data regulation, shifting from a fragmented, sectoral model toward a comprehensive legislative framework governing personal data processing. While the Act seeks to institutionalize consent-based data governance and provide enforceable rights to data principals, it simultaneously expands the scope of State exemptions and executive discretion, particularly in areas relating to governance, security, and public order. This section situates the DPDP Act within the broader evolution of data protection discourse in India and identifies the central research problem addressed in this paper: whether the Act successfully reconciles the constitutional imperative of protecting privacy with the expanding authority of the State in the digital age. The analysis interrogates whether the legislative framework strikes an appropriate balance between individual rights and State power or whether it risks normalizing surveillance and diluting constitutional safeguards under the guise of digital governance and administrative efficiency.

III. Evolution of Data Protection Law in India

The development of data protection norms in India has been gradual, fragmented, and largely reactive, shaped by technological change, judicial intervention, and policy experimentation rather than a unified legislative vision. Prior to the enactment of the Digital Personal Data Protection Act, 2023, India lacked a comprehensive statutory framework dedicated to the protection of personal data. Instead, data protection obligations were embedded within the broader framework of cyber regulation under the Information

Technology Act, 2000. The Act primarily addressed issues of electronic commerce, cybercrime, and intermediary liability, offering only limited and indirect safeguards for personal data. Provisions such as Section 43A, which imposed compensation liability for failure to protect sensitive personal data, and Section 72A, which criminalized breach of confidentiality, reflected a narrow, harm-based approach rather than a rights-oriented conception of privacy. These limited protections were supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. While the Rules introduced obligations relating to consent, purpose limitation, and reasonable security practices, their scope was confined to corporate entities and excluded State agencies from their ambit. Moreover, the Rules suffered from weak enforcement mechanisms, vague standards, and a lack of independent oversight, rendering them inadequate in the face of large-scale data collection by both public and private actors. As a result, data protection in India remained largely procedural and contractual, rather than constitutional and rights-based.

A transformative shift occurred with the Supreme Court's landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017), which fundamentally reoriented the discourse on privacy and data protection. By recognizing privacy as a fundamental right under Article 21, the Court underscored the intrinsic link between informational autonomy, human dignity, and democratic participation. Importantly, the judgment established a structured constitutional test requiring any restriction on privacy to satisfy the requirements of legality, legitimate State aim, proportionality, and procedural safeguards against abuse. This decision not only invalidated the notion of privacy as a purely statutory or common law interest but also imposed a positive obligation on the State to enact a comprehensive data protection regime. In response to this constitutional mandate, the Government of India constituted the Committee of Experts under the chairmanship of Justice B.N. Srikrishna, which submitted its report titled A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians in 2018. The Srikrishna Committee articulated a robust rights-based framework for data protection, drawing heavily from comparative global standards such as the European Union's General Data Protection Regulation (GDPR). The report emphasized principles of consent, purpose limitation, data minimization, transparency, and accountability, while also advocating for the establishment of an independent Data Protection Authority insulated from executive control. At the same time, it cautioned against broad and unchecked State exemptions, recommending that any derogation from data protection obligations must conform to constitutional proportionality standards.

The Personal Data Protection Bill, 2019, introduced in Parliament based largely on the Srikrishna Committee's recommendations, marked India's first serious legislative attempt to codify comprehensive data protection norms. However, the Bill attracted significant criticism for expanding State surveillance powers, permitting wide exemptions for government agencies, and diluting the independence of the proposed regulatory authority. These concerns intensified during parliamentary scrutiny, leading to multiple revisions and delays. The subsequent withdrawal of the 2019 Bill signaled a shift in the government's regulatory approach. This shift became more evident with the introduction of the Digital Personal Data Protection Bill, 2022, which adopted a significantly streamlined and minimalist structure. While the 2022 Bill simplified compliance obligations and narrowed the scope of regulation to digital personal data, it also expanded executive discretion by empowering the State to exempt government agencies from the application of the law on broad grounds such as public order and national security. The Bill further reduced

institutional safeguards by replacing the independent Data Protection Authority with a Data Protection Board whose members were to be appointed and controlled by the executive.

These legislative trajectories culminated in the enactment of the Digital Personal Data Protection Act, 2023. The final Act reflects the evolution and dilution of India's data protection framework, balancing economic efficiency and administrative flexibility against individual privacy rights. While the Act institutionalizes certain core data protection principles and introduces penalties for non-compliance, it also embeds extensive State exemptions and centralizes regulatory power within the executive. This section thus demonstrates how earlier concerns regarding surveillance, regulatory independence, and proportionality not only persisted but became structurally embedded in the 2023 Act, raising critical questions about its constitutional adequacy and long-term impact on privacy governance in India.

IV. Constitutional Right to Privacy and Data Protection

Indian privacy jurisprudence underwent a profound constitutional transformation with the Supreme Court's unanimous judgment in Justice K.S. Puttaswamy v. Union of India (2017), which recognized the right to privacy as an intrinsic component of the right to life and personal liberty under Article 21, as well as an emanation of other fundamental freedoms guaranteed by Part III of the Constitution. Prior to Puttaswamy, privacy protections in India were fragmented and uncertain, oscillating between statutory interpretation and common law reasoning. The judgment decisively rejected this ambiguity by affirming privacy as a foundational constitutional value essential to individual dignity, autonomy, and democratic participation. A central contribution of the Puttaswamy decision lies in the articulation of a structured constitutional framework governing State action that infringes upon privacy. The Court held that any limitation on the right to privacy must satisfy four cumulative requirements: legality, legitimate State aim (often articulated as necessity), proportionality, and the existence of procedural safeguards against abuse. The requirement of legality mandates that any intrusion into privacy must be authorized by law, thereby precluding executive or administrative actions unsupported by legislative sanction. This principle ensures democratic accountability and guards against arbitrary State interference.

The requirement of necessity demands that the State demonstrate a legitimate objective of sufficient importance, such as national security, public order, or welfare administration, to justify restrictions on privacy. Importantly, the Court clarified that mere administrative convenience or speculative benefits cannot constitute valid grounds for curtailing fundamental rights. This principle establishes a threshold of justification that data protection legislation must meet when permitting data collection, processing, or surveillance by the State. Proportionality occupies a pivotal role in the constitutional analysis of privacy infringements. Drawing from comparative constitutional jurisprudence, the Court emphasized that State measures must bear a rational nexus to the stated objective, must be the least restrictive means available, and must strike a fair balance between individual rights and competing public interests. In the context of data protection, proportionality requires that data collection be limited in scope, duration, and purpose, and that intrusive technologies such as mass surveillance or profiling be subjected to heightened scrutiny. Overbroad or blanket exemptions allowing unrestricted data processing by the State would thus fail the proportionality test.

Equally significant is the requirement of procedural safeguards, which seeks to prevent abuse of power by ensuring transparency, oversight, and accountability. The Court underscored the need for independent review mechanisms, access to remedies, and safeguards such as notice, consent, and judicial or quasi-judicial authorization in cases involving

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

intrusive data processing. These safeguards are particularly crucial in an era of algorithmic governance, where automated decision-making can obscure accountability and exacerbate power asymmetries between the State and individuals. Beyond these structural principles, Puttaswamy located privacy within a broader normative framework grounded in dignity, autonomy, and informational self-determination. The Court recognized that control over personal data is integral to an individual's ability to shape their identity, exercise freedom of choice, and participate meaningfully in social and political life. Informational privacy, in this sense, extends beyond secrecy and encompasses the right to determine how personal data is collected, used, and disseminated. This conception aligns Indian constitutional jurisprudence with global data protection norms that emphasize individual control and accountability.

The judgment also delineates constitutional limits on State surveillance and data processing. While acknowledging that the State may legitimately collect and process personal data for governance and security purposes, the Court cautioned against the normalization of surveillance and the creation of a "surveillance State" incompatible with constitutional democracy. Any data-driven governance model must therefore be narrowly tailored, transparently regulated, and subject to independent oversight. In this framework, comprehensive data protection legislation assumes a constitutional function, serving as the primary instrument through which the State operationalizes its obligation to respect, protect, and fulfill the right to privacy. This section thus establishes Puttaswamy as the constitutional touchstone against which the Digital Personal Data Protection Act, 2023 must be evaluated. The principles articulated in the judgment operate not merely as interpretive guidelines but as binding constitutional benchmarks that determine the validity of legislative choices relating to data governance, State surveillance, and individual rights in the digital age.

V. Overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 establishes the first comprehensive statutory framework in India governing the processing of digital personal data. The Act is designed to regulate the collection, use, storage, and disclosure of personal data by both State and non-State actors, while simultaneously facilitating lawful data processing for governance, innovation, and economic activity. This section provides a structured overview of the Act's architecture, key definitions, regulatory mechanisms, and institutional arrangements, forming the foundation for a critical evaluation of its constitutional adequacy. At the definitional level, the Act adopts a broad understanding of "personal data" as any data about an individual who is identifiable by or in relation to such data, provided the data is processed in digital form or digitized subsequently. This expansive definition reflects contemporary data realities, where even ostensibly anonymized datasets can enable identification through aggregation and inference. The Act identifies the individual to whom the data relates as the "data principal," recognizing them as the primary rights-holder under the statute. Entities that determine the purpose and means of processing personal data are designated as "data fiduciaries," a term that signifies a duty of trust and responsibility toward data principals. In addition, the Act introduces the concept of "consent managers," registered entities authorized to enable data principals to manage, review, and withdraw consent through interoperable platforms, thereby institutionalizing consent as a continuous and dynamic process rather than a one-time transaction.

A central feature of the DPDP Act is its consent-based framework for lawful data processing. Consent must be free, specific, informed, unconditional, and unambiguous, and must be given through a clear affirmative action. The Act requires that data fiduciaries provide notice specifying the purpose of data collection, the

nature of personal data processed, and the rights available to data principals. While this framework aligns in principle with global data protection norms, the Act permits non-consensual processing in several circumstances, including for State functions, compliance with law, and public interest purposes. These exceptions significantly shape the balance between individual autonomy and State authority, and their breadth has important constitutional implications. The Act imposes a range of obligations on data fiduciaries to ensure responsible data governance. These include the duty to process personal data only for lawful purposes, to implement reasonable security safeguards to prevent data breaches, and to ensure the accuracy and completeness of data where such accuracy is necessary for the intended purpose. Data fiduciaries are also required to delete personal data once the purpose for which it was collected has been fulfilled, unless retention is required by law. Certain entities may be notified as "significant data fiduciaries" based on factors such as volume and sensitivity of data processed, and are subject to heightened obligations, including the appointment of a data protection officer and the conduct of periodic data protection impact assessments.

The DPDP Act grants data principals a set of statutory rights intended to operationalize informational self-determination. These include the right to access information about personal data processed, the right to correction and erasure of inaccurate or outdated data, the right to grievance redressal, and the right to nominate another individual to exercise these rights in the event of incapacity or death. However, unlike some global frameworks, the Act does not recognize certain advanced rights such as data portability or the right to object to automated decision-making, thereby limiting the scope of individual control over data. With respect to cross-border data transfers, the Act adopts a permissive approach by allowing the transfer of personal data outside India to such countries or territories as may be notified by the Central Government. This marks a departure from earlier data localization proposals and reflects a policy choice favoring global data flows and economic integration. However, the absence of statutory criteria or adequacy standards for determining permissible jurisdictions raises concerns regarding transparency, reciprocity, and protection against foreign surveillance regimes. Enforcement of the DPDP Act is primarily vested in the Data Protection Board of India, which functions as the central adjudicatory authority under the statute. The Board is empowered to inquire into complaints, direct remedial measures, impose monetary penalties, and enforce compliance with the Act. However, the role, composition, and appointment process of the Board raise significant questions about institutional independence. Members of the Board are appointed by the Central Government, and the Act does not provide for judicial participation or security of tenure comparable to independent regulatory bodies. This institutional design has been criticized for concentrating excessive control in the executive, potentially undermining the Board's ability to act as an impartial guardian of privacy rights, particularly in cases involving State data processing. Penalties for non-compliance under the Act are substantial, with monetary fines extending up to several hundred crore rupees, depending on the nature and severity of the violation.

VI. State Power and Exemptions under the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 contains several provisions that permit the State to exempt itself from the application of data protection obligations on grounds such as national security, public order, and the performance of governmental functions. While the recognition of limited derogations for legitimate State interests is consistent with constitutional doctrine and comparative global practice, the breadth and structure of these exemptions raise serious concerns regarding their compatibility with constitutional standards

of necessity, proportionality, and procedural restraint. At the constitutional level, any restriction on the right to privacy must satisfy the four-fold test articulated by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*, namely legality, legitimate State aim, proportionality, and procedural safeguards against abuse. Although the DPDP Act satisfies the requirement of legality by providing statutory authorization for exemptions, the remaining elements of this constitutional test are insufficiently addressed. The grounds on which exemptions may be granted-such as national security, public order, and governance-are framed in broad and indeterminate terms, leaving substantial room for expansive interpretation. The absence of precise statutory definitions or objective criteria undermines the requirement of necessity, as it becomes difficult to assess whether data processing is genuinely required to achieve a legitimate State objective.

The proportionality of State exemptions under the Act is further weakened by the lack of internal limitations on the scope, duration, and intensity of exempted data processing activities. The Act does not mandate that exemptions be narrowly tailored or restricted to the least intrusive means available. Nor does it require periodic review or sunset clauses to reassess the continued justification for such exemptions. In contrast, constitutional jurisprudence demands that privacy-infringing measures be calibrated to minimize harm and avoid excessive intrusion. The absence of such safeguards increases the risk that exemptions will operate as blanket authorizations for large-scale data collection and retention. Executive discretion plays a dominant role in the exemption regime established by the Act. The Central Government is empowered to determine when and how exemptions apply, with minimal statutory guidance and no requirement for independent authorization. This concentration of power within the executive branch raises concerns regarding arbitrariness and undermines the principle of separation of powers. From a constitutional standpoint, unchecked executive discretion in matters involving fundamental rights is inherently problematic, particularly where the same authority that collects and processes data also determines the limits of its own obligations.

The lack of meaningful judicial oversight further compounds these concerns. The Act does not provide for prior judicial approval or ex post facto judicial review of exemption orders, nor does it require transparency in the invocation of exemptions. Individuals affected by exempted data processing may have limited awareness of, or ability to challenge, such actions. This absence of judicial scrutiny contrasts sharply with established constitutional safeguards governing surveillance and data interception, where courts have emphasized the importance of independent oversight to prevent abuse. Perhaps the most significant risk arising from these exemptions is the potential normalization of mass surveillance. In an environment characterized by interoperable government databases, advanced analytics, and artificial intelligence, broad exemptions can facilitate continuous monitoring, profiling, and aggregation of personal data across multiple domains of an individual's life. Without clear legal constraints and oversight, such practices threaten to erode the core values of privacy, autonomy, and democratic participation. The chilling effect on speech, association, and political dissent further underscores the democratic implications of an inadequately constrained exemption regime. Taken together, these factors call into question whether the DPDP Act effectively restrains State power over personal data. While the pursuit of national security and effective governance is undoubtedly legitimate, constitutional fidelity requires that such objectives be pursued within a framework that rigorously limits intrusion into fundamental rights. The current exemption provisions, as structured, tilt the balance decisively in favor of executive authority, risking the transformation of data protection law into an instrument of surveillance rather than a

safeguard against it. A reconfiguration of these provisions, grounded in proportionality, necessity, and judicial oversight, is therefore essential to align the Act with constitutional privacy standards.

VII. Compliance with Global Data Protection Norms

A comparative evaluation of the Digital Personal Data Protection Act, 2023 alongside established global data protection frameworks reveals both normative convergence and significant structural divergence. International instruments such as the European Union's General Data Protection Regulation (GDPR), the United Kingdom's Data Protection Act, 2018, and the OECD Privacy Guidelines provide widely accepted benchmarks for assessing the adequacy of domestic data protection regimes. These frameworks are grounded in rights-based regulation, institutional independence, and accountability, offering a useful lens through which the Indian data protection framework may be critically examined. With regard to consent, the DPDP Act reflects alignment with global standards by recognizing consent as a central basis for lawful data processing and by prescribing requirements of clarity, specificity, and informed choice. Similar formulations are found in the GDPR and the UK framework, where consent must be freely given and capable of withdrawal. However, a key point of divergence lies in the scope of non-consensual processing permitted under Indian law. While the GDPR allows processing without consent only under narrowly defined lawful bases subject to strict proportionality and oversight, the DPDP Act permits wide-ranging exemptions for State functions, public interest, and governance-related purposes. Principles of data minimization and purpose limitation occupy a foundational position in global data protection law. Under the GDPR, these principles operate as enforceable constraints requiring that personal data be limited to what is strictly necessary and processed only for specified, legitimate purposes. Compliance is reinforced through mandatory accountability tools such as data protection impact assessments and detailed record-keeping obligations. Although the DPDP Act incorporates similar principles in its statutory language, their application remains uneven. Broad exemptions granted to government agencies and the absence of mandatory impact assessments for State-led data processing reduce the practical enforceability of these safeguards, increasing the risk of excessive data collection and repurposing. Institutional independence constitutes one of the most pronounced points of divergence between the Indian regime and global norms. The GDPR mandates the establishment of independent supervisory authorities insulated from political influence, with guaranteed autonomy in appointments, tenure, and decision-making. The UK Information Commissioner's Office similarly operates as an independent regulator accountable to Parliament. In contrast, the Data Protection Board of India is structurally situated within the executive domain, with appointments, service conditions, and removal processes controlled by the Central Government. This institutional design raises concerns regarding impartial enforcement, particularly in cases involving alleged violations by State agencies.

The availability of effective remedies further differentiates the Indian framework from international standards. Global data protection regimes recognize the right to an effective remedy as integral to privacy protection, allowing individuals to seek compensation for both material and non-material harm resulting from unlawful data processing. The GDPR explicitly provides for judicial remedies and regulatory enforcement independent of executive discretion. The DPDP Act, while providing for monetary penalties and grievance redressal mechanisms, does not expressly recognize a right to compensation for privacy violations, nor does it establish a robust appellate structure independent of executive oversight. This limitation constrains individual access to justice and weakens the deterrent effect of the law. The OECD Privacy Guidelines

adopt a principles-based approach emphasizing accountability, transparency, and proportional safeguards, particularly in relation to governmental data use. While the DPDP Act aligns with the OECD's emphasis on regulatory flexibility and innovation, it falls short in embedding accountability mechanisms capable of effectively constraining State power. The limited articulation of checks on governmental data processing contrasts with the OECD's emphasis on proportionality and oversight.

Overall, the comparative analysis demonstrates that although the DPDP Act, 2023 incorporates several internationally recognized data protection principles, it departs from global norms in its treatment of State accountability and regulatory independence. The framework privileges administrative discretion and governance efficiency over enforceable rights and institutional safeguards, resulting in a comparatively weaker protection regime. These divergences have significant implications for constitutional compliance, cross-border data transfers, and India's credibility within the global data protection landscape.

VIII. Institutional Framework and Enforcement Challenges

The institutional design of the Data Protection Board of India occupies a central position in the enforcement architecture of the Digital Personal Data Protection Act, 2023, as it functions as the primary adjudicatory and regulatory body responsible for ensuring compliance with the statutory framework. An analysis of the structure, powers, and operational autonomy of the Board is therefore essential to assess the effectiveness of the data protection regime and its conformity with constitutional and global standards of independent regulation. Under the DPDP Act, the Data Protection Board of India is constituted by the Central Government, which is vested with the authority to appoint the Chairperson and other members of the Board, as well as to determine their qualifications, tenure, terms of service, and conditions of removal. This appointment process reflects a high degree of executive involvement, with no mandatory role assigned to the judiciary, Parliament, or an independent selection committee. In contrast to global best practices, where data protection authorities are insulated from political influence through fixed tenure and transparent appointment procedures, the Indian model concentrates significant institutional control within the executive. This raises concerns regarding the Board's ability to function as an impartial and independent regulator, particularly in matters involving alleged violations by State agencies or government instrumentalities.

The powers of the Data Protection Board are primarily adjudicatory and enforcement-oriented. The Board is empowered to inquire into complaints, direct remedial measures, impose monetary penalties for non-compliance, and enforce obligations under the Act. These powers are significant in scale, especially given the substantial financial penalties prescribed under the statute. However, the effectiveness of these powers is closely linked to the Board's independence and procedural safeguards. The absence of clearly defined investigative autonomy and the reliance on executive-controlled processes may undermine the Board's capacity to act decisively against powerful data fiduciaries, including State actors. Accountability mechanisms governing the Board further complicate its institutional position. While the Board is expected to function in a manner consistent with principles of natural justice, the Act does not provide detailed procedural guidelines for inquiries, hearings, or evidence evaluation. Moreover, reporting and oversight mechanisms remain largely executive-driven, with limited parliamentary scrutiny. This framework contrasts with international models where supervisory authorities are accountable to legislatures and subject to judicial review, thereby ensuring a balance between independence and democratic oversight.

A particularly significant limitation of the DPDP Act lies in its appellate and remedial structure. Decisions of the Data Protection Board are appealable to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), a body whose primary expertise lies in telecommunications regulation rather than data protection or constitutional rights. This choice of appellate forum raises concerns regarding subject-matter competence and accessibility for data principals, particularly individual users seeking redress for privacy violations. Additionally, the absence of an explicit statutory right to compensation for harm suffered as a result of unlawful data processing limits the remedial options available to affected individuals, reducing the law's deterrent and restorative impact. From the perspective of access to justice, the DPDP Act places significant procedural and practical burdens on data principals. The grievance redressal process requires individuals to first approach data fiduciaries before escalating complaints to the Board, potentially discouraging reporting in cases involving large corporations or State agencies. Combined with the lack of decentralized enforcement mechanisms and limited public awareness of data protection rights, these structural constraints may impede effective implementation of the law. Practical challenges in implementation further compound these institutional concerns. The Board is expected to regulate a vast and diverse digital ecosystem encompassing government departments, multinational corporations, and small enterprises. Without adequate resources, technical expertise, and operational autonomy, the Board may struggle to discharge its functions effectively. The absence of clear timelines for adjudication and the reliance on executive notifications for key procedural aspects introduce uncertainty and may weaken regulatory predictability.

In sum, while the Data Protection Board of India is envisaged as the cornerstone of enforcement under the DPDP Act, its current institutional design raises serious concerns regarding independence, accountability, and access to remedies. The concentration of executive control, limited appellate safeguards, and practical implementation challenges risk undermining the Board's effectiveness as a guardian of privacy rights. Strengthening the Board's autonomy, enhancing procedural protections, and expanding remedial avenues are therefore critical to ensuring that the data protection framework operates as a meaningful check on both State and private power in the digital age.

IX. Implications for Digital Governance and Civil Liberties

The Digital Personal Data Protection Act, 2023 has far-reaching implications for India's digital governance framework, extending beyond individual privacy to shape the relationship between the State, private actors, and citizens in the digital public sphere. By formalizing rules for data collection and processing, the Act directly influences how power is exercised through data-driven governance, surveillance infrastructures, and platform-based decision-making. Its impact must therefore be assessed not only in terms of compliance and enforcement but also in relation to democratic accountability, freedom of expression, and the distribution of informational power in society. From the perspective of digital governance, the Act institutionalizes large-scale data processing as a legitimate tool of administration and policy implementation. Government databases linked to welfare delivery, identity verification, and public service platforms rely heavily on personal data aggregation and interoperability. While the Act provides legal authorization for such processing, the breadth of exemptions available to the State risks normalizing expansive data collection with limited oversight. This raises concerns about function creep, whereby data collected for specific administrative purposes may be repurposed across agencies, enabling comprehensive profiling of individuals. In the absence of strict proportionality limits and independent review mechanisms, digital governance may evolve in ways that prioritize

efficiency and control over constitutional safeguards.

The implications for surveillance are particularly significant. The DPDP Act permits non-consensual data processing by the State for broadly framed objectives such as public order, security, and governance. When combined with advanced analytics, artificial intelligence, and interconnected databases, these provisions may facilitate continuous and opaque forms of surveillance. Such practices risk undermining the constitutional guarantee of privacy and may produce a chilling effect on individual behavior, particularly in contexts involving political participation, dissent, and association. Surveillance enabled through lawful data processing, when insufficiently constrained, can alter the balance between citizen and State, shifting democratic governance toward a model of administrative monitoring rather than participatory accountability. The Act also has important consequences for freedom of expression in the digital ecosystem. Profiling, content moderation, and algorithmic decision-making by technology platforms increasingly rely on personal data to curate information, target speech, and regulate online behavior. While the DPDP Act imposes certain obligations on data fiduciaries, it does not explicitly address the risks posed by automated decision-making systems, including bias, opacity, and lack of explainability. In the absence of rights to object to profiling or to seek explanations for automated decisions, individuals may find their expressive freedoms indirectly constrained through data-driven filtering and visibility controls exercised by both platforms and State actors.

For private entities and technology platforms, the Act introduces compliance obligations that reshape data governance practices, including consent management, security safeguards, and data retention limits. While these obligations may enhance accountability, the discretionary enforcement structure and differential treatment of State and private actors create an uneven regulatory landscape. Private platforms may be subject to stringent penalties and compliance burdens, while State agencies operating large-scale databases enjoy broad exemptions, raising concerns about regulatory asymmetry and competitive neutrality. This imbalance may also incentivize excessive data sharing with government agencies, potentially eroding user trust. From the standpoint of democratic accountability, the DPDP Act's approach to data governance places significant reliance on executive discretion, with limited transparency and external oversight. Democratic accountability in the digital age requires that citizens have meaningful avenues to challenge data-driven decisions, understand how their data is used, and hold both State and private actors accountable for misuse. The Act's limited remedial framework, absence of explicit protections against profiling and automated decision-making, and weak institutional independence constrain the realization of these democratic ideals. Overall, the DPDP Act, 2023 reshapes India's digital governance architecture in ways that extend beyond privacy protection. While it provides a formal legal basis for data regulation in an increasingly digitized society, it simultaneously raises concerns regarding surveillance, expressive freedom, and democratic accountability. The Act's long-term impact will depend on how its provisions are interpreted, enforced, and supplemented by institutional safeguards capable of ensuring that data-driven governance remains consistent with constitutional values and democratic norms.

X. Critical Assessment and Key Gaps

The Digital Personal Data Protection Act, 2023 reflects a significant legislative intervention in India's digital regulatory landscape, yet a holistic assessment of its design and operation reveals a number of structural and normative shortcomings that undermine its capacity to fully realize the constitutional promise of privacy. When examined collectively, these limitations indicate a regulatory framework that prioritizes administrative flexibility and State authority over robust, rights-based data

protection. A central weakness of the Act lies in the dilution of consent as a meaningful safeguard for informational autonomy. Although the statute formally adopts consent as the primary basis for lawful data processing, the breadth of statutory exceptions substantially erodes its practical significance. Consent is rendered secondary in a wide range of contexts involving State functions, compliance with law, and broadly defined public interest purposes. Unlike constitutional privacy jurisprudence, which requires that non-consensual intrusions satisfy strict necessity and proportionality tests, the Act does not embed comparable substantive thresholds or procedural safeguards. As a result, consent risks becoming a formalistic requirement rather than an effective mechanism of individual control over personal data.

Closely linked to this concern is the expansive scope of State exemptions under the Act. The Central Government is empowered to exempt government agencies from the application of the law on grounds such as national security, public order, and governance. These grounds are framed in broad and indeterminate terms, granting wide discretionary authority to the executive. The absence of statutory criteria, temporal limits, or independent oversight mechanisms governing such exemptions raises the possibility of routine and normalized departures from data protection obligations. From a constitutional perspective, these exemptions sit uneasily with the proportionality and necessity standards articulated in *Justice K.S. Puttaswamy v. Union of India*, particularly given the potential for large-scale surveillance and profiling enabled by modern data technologies.

The lack of an independent regulatory authority further weakens the protective architecture of the Act. The Data Protection Board of India, while vested with enforcement powers, is institutionally embedded within the executive framework, with appointments, service conditions, and removal processes controlled by the Central Government. This structural dependence compromises the Board's ability to function as a neutral and impartial adjudicator, especially in cases involving State data processing. Comparative global frameworks underscore the importance of regulatory independence as a cornerstone of effective data protection, a standard that the Indian framework does not adequately meet. Judicial oversight and access to remedies under the Act are similarly constrained. The absence of a clearly articulated right to compensation for privacy violations limits the remedial options available to data principals. Moreover, the appellate mechanism, which channels appeals to a specialized tribunal with limited expertise in constitutional and privacy law, restricts meaningful judicial scrutiny of executive action. These limitations weaken the enforceability of privacy rights and reduce the deterrent effect of the law, particularly in relation to powerful State and corporate actors.

Taken together, these shortcomings raise a fundamental question regarding the normative orientation of the DPDP Act, 2023. While the Act represents a formal acknowledgment of the need for data protection in a digital society, its design suggests a regulatory model more closely aligned with the consolidation of State control over data than with the robust protection of individual rights. The extensive reliance on executive discretion, coupled with limited institutional and judicial checks, risks transforming data protection law into an instrument of governance rather than a shield against arbitrary power. In evaluating whether the Act fulfills the constitutional promise of privacy, it becomes evident that the framework falls short of the standards articulated by the Supreme Court. The right to privacy, as understood in Indian constitutional jurisprudence, demands not only legal recognition but also effective safeguards capable of constraining State power and preserving individual autonomy. Without substantial reforms aimed at strengthening consent, narrowing State exemptions, ensuring regulatory independence, and enhancing

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

judicial oversight, the DPDP Act remains an incomplete realization of this constitutional mandate.

XI. Recommendations and Legal Reforms

The deficiencies identified in the Digital Personal Data Protection Act, 2023 necessitate a recalibration of the legal framework to ensure that data protection functions as a meaningful constitutional safeguard rather than a formal regulatory mechanism. Any reform agenda must be guided by the principles articulated in Indian privacy jurisprudence and informed by comparative global best practices, particularly those embedded in mature data protection regimes. Strengthening the Act requires a shift from executive-centric governance toward rights-based regulation anchored in accountability, proportionality, and institutional independence. A primary area for reform concerns the scope of State exemptions. The existing provisions allowing broad exemptions for governmental data processing on grounds such as national security, public order, and governance require substantial narrowing. Comparative frameworks, including the GDPR and the UK Data Protection Act, permit derogations for State functions only where they are strictly necessary, clearly defined, and accompanied by safeguards. Indian law would benefit from adopting similar statutory constraints, including precise definitions, purpose-specific limitations, temporal boundaries, and mandatory periodic review of exemptions. Embedding a requirement of demonstrable necessity and proportionality within the text of the statute would align State data processing with constitutional standards and reduce the risk of arbitrary surveillance.

Closely related is the need to strengthen proportionality safeguards across the data protection framework. Legislative authorization alone is insufficient to justify intrusive data practices in the absence of substantive limitations and procedural checks. Comparative best practices emphasize the use of data protection impact assessments, particularly for high-risk processing such as profiling, biometric identification, and large-scale government databases. Introducing mandatory impact assessments for State-led data processing, coupled with public disclosure and independent review, would enhance transparency and ensure that privacy-intrusive measures are subject to reasoned justification. Reform of the institutional framework governing enforcement is equally critical. The independence of the Data Protection Board of India must be structurally guaranteed to ensure impartial adjudication and credible oversight. Global data protection regimes uniformly recognize independent supervisory authorities as essential to effective enforcement. Reforms could include the establishment of a transparent, multi-stakeholder appointment process involving the judiciary or Parliament, fixed tenure for Board members, and statutory protection against arbitrary removal. Financial and operational autonomy would further insulate the Board from executive influence and enhance public confidence in its decisions.

Enhancing transparency obligations represents another important reform priority. Data protection regimes in the European Union and the United Kingdom impose rigorous disclosure requirements on both public and private entities, including obligations to explain data processing practices, automated decision-making systems, and data-sharing arrangements. Incorporating stronger transparency provisions within the DPDP Act, particularly for State agencies, would empower individuals to understand and challenge the use of their personal data. This is especially relevant in the context of algorithmic governance, where opacity can obscure accountability and entrench power asymmetries. Finally, the introduction of stronger and more accessible remedies for individuals is essential to realizing the right to privacy in practice. Comparative frameworks recognize the right to compensation for both material and non-material harm arising from unlawful data processing, alongside robust

judicial remedies. Indian law would benefit from explicitly recognizing a statutory right to compensation and from simplifying access to courts for privacy-related grievances. Expanding appellate review by constitutional courts and strengthening procedural safeguards would reinforce the deterrent effect of the law and ensure meaningful access to justice for data principals. Taken together, these reforms would move the DPDP Act closer to global best practices and constitutional expectations. By narrowing State exemptions, strengthening proportionality safeguards, ensuring institutional independence, enhancing transparency, and expanding individual remedies, the data protection framework can be reoriented toward protecting individual autonomy and democratic accountability. Such recalibration is essential if data protection law in India is to function not merely as a tool of digital governance, but as a substantive constitutional guarantee in the digital age.

XII. Conclusion

The analysis undertaken in this paper leads to the conclusion that although the Digital Personal Data Protection Act, 2023 marks an important milestone in India's journey toward regulating personal data, it does not fully satisfy the constitutional and normative expectations that flow from the recognition of privacy as a fundamental right. The enactment of a comprehensive data protection statute addresses a long-standing legislative gap and signals the State's acknowledgment of the centrality of privacy in a digital society. However, the substantive design and institutional architecture of the Act reveal persistent tensions between the protection of individual rights and the consolidation of State authority over data. From a constitutional perspective, the Act falls short of the standards articulated by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*, particularly with respect to necessity, proportionality, and procedural safeguards. The breadth of State exemptions, diluted consent requirements, and limited avenues for independent oversight weaken the Act's capacity to meaningfully restrain intrusive data practices. Rather than operating as a robust rights-based framework, the law risks normalizing expansive data collection and surveillance under the rubric of governance, security, and administrative efficiency.

When assessed against global data protection norms, the divergences become more pronounced. While the DPDP Act incorporates several internationally recognized principles in form, it departs from best practices in substance, especially in relation to regulatory independence, State accountability, and access to effective remedies. The concentration of enforcement authority within an executive-controlled body and the absence of strong judicial safeguards limit the law's ability to provide effective protection against both governmental and corporate misuse of personal data.

The paper therefore concludes that meaningful data protection in India requires a recalibration of the existing framework. Narrowing the scope of State power, embedding proportionality and necessity as enforceable statutory standards, strengthening the independence of the Data Protection Board, and expanding individual remedies are essential reforms if the law is to fulfill its constitutional promise. Without such recalibration, data protection risks becoming an instrument of control rather than a safeguard of autonomy. Ultimately, the future of data protection in India will depend on whether the legal framework evolves to place individual dignity, autonomy, and democratic accountability at its core. A data protection regime that genuinely protects privacy has the potential to strengthen public trust in digital governance and reinforce democratic values. Conversely, a framework that enables unchecked surveillance and executive dominance threatens to erode the very constitutional foundations it purports to protect.

References

[1] Bennett, C. J., & Raab, C. D. (2020). The governance of privacy: Policy instruments in global perspective (2nd ed.). MIT Press.

[2] Bhandari, V. (2023). India's Digital Personal Data Protection Act, 2023: A preliminary constitutional critique. Indian Journal of Law and Technology, 19(2), 1–28.

[3] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, India.

[4] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

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

[6] Kuner, C., Bygrave, L. A., & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.

[7] Law Commission of India. (2018). Consultation paper on data protection. Government of India.

[8] Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. OECD Publishing.

[8] Srikrishna, B. N. (2018). A free and fair digital economy: Protecting privacy, empowering Indians (Report of the Committee of Experts on Data Protection Framework for India). Government of India.

[9] Solove, D. J. (2021). Understanding privacy (2nd ed.). Harvard University Press.

[10] State of West Bengal v. Anwar Ali Sarkar, AIR 1952 SC 75 (India).

[11] United Nations High Commissioner for Human Rights. (2018). The right to privacy in the digital age (A/HRC/39/29).

[12] Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453.

[13] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

[14] Bhatia, G. (2019). The transform-ative Constitution: A radical biography in nine acts. HarperCollins India.

[15] Bhatia, G. (2023). Surveillance, proportionality, and India's data protection law. National Law School of India Review, 35(1), 1–24.

[16] Centre for Internet and Society. (2023). A critique of the Digital Personal Data Protection Act, 2023. CIS Policy Brief.

[17] European Court of Human Rights. (1978). Klass and Others v. Germany, App. No. 5029/71.

[18] Justice K.S. Puttaswamy (Aadhaar–5J.) v. Union of India, (2019) 1 SCC 1 (India).

[19] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

[20] Kuner, C. (2015). Reality and illusion in EU data transfer regulation post Schrems. German Law Journal, 18(4), 881–918.

[21] Ohlin, J. D. (2020). The right to privacy and the surveillance state. Harvard International Law Journal, 61(2), 345–392.

[22] Privacy International. (2021). Government hacking and surveillance: Legal safeguards and human rights. PI Report.

[23] Srikrishna, B. N. (2023). Data protection and the limits of State power. Indian Journal of Constitutional Law, 17(2), 45–68.

[24] Solove, D. J. (2011). Nothing to hide: The false tradeoff between privacy and security. Yale University Press.