A CRITICAL ANALYSIS OF THE ISSUES AND PRACTICAL CHALLENGES IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Prakhar Dwivedi, Barkatullah University, Bhopal

Rohit Kumar Chaturvedi, Barkatullah University, Bhopal

ABSTRACT

India's first comprehensive legal framework for controlling the processing of personal data is the Digital Personal Data Protection Act, 2023 (DPDPA). The Act aims to create a consent-based data protection framework and was enacted following the Supreme Court's recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India. This study contends that although the DPDPA represents a formal advancement, its ability to safeguard rights is undermined by significant and fundamental flaws by means of a doctrinal examination of important clauses, such as Sections 7, 8, 9, 17, 20, and 37. This paper shows that the Act increases the power of the executive to make decisions, weakens the independence of regulatory bodies, and gets rid of important protections for transparency, such as the public interest override that was possible under the Right to Information Act.

The State's extensive exemptions, the lack of impartial oversight of enforcement, and the unbridled authority to block digital platforms are all highlighted in particular. Based on constitutional principles and comparative frameworks like the General Data Protection Regulation (GDPR) of the European Union, the paper argues that the DPDPA does not meet the necessary, proportional, and accountable thresholds required by Indian constitutional jurisprudence. The report concludes by suggesting changes to the law that would restore democratic protections and bring India's data protection laws into compliance with international standards.

Keywords: Data privacy, Right to Information, Transparency, accountability, Data fiduciary, Public interest, etc.

INTRODUCTION

In India's quest to establish a thorough data protection system, the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) represents a critical turning point. The Act was created to protect informational autonomy in the digital age after the Supreme Court recognised the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India. Notwithstanding its professed goal of empowering people and encouraging responsible data governance, the DPDPA raises significant issues with regard to the over-concentration of executive power, the dilution of transparency, and the deterioration of accountability.

Through the lens of democratic rights, this study critically analyses the DPDPA, emphasising how various provisions—specifically Sections 7, 8, 9, 17, 20, 37, and others—either deteriorate the right to information, grant the State unrestricted exemptions, or erode institutional safeguards. The elimination of the Right to Information Act's public interest override, the lack of impartial oversight procedures, the ambiguity of enforcement schedules, and the executive branch's broad authority to grant exemptions and block platforms are some of the main causes for concern.

The study also identifies doctrinal and structural flaws in the DPDPA, including the Central Government's disproportionate discretionary power in government accountability and the lack of a category for sensitive personal data. It also assesses whether Indian law satisfies international and constitutional requirements for privacy and due process by contrasting these provisions with international norms, such as the General Data Protection Regulation (GDPR) of the EU.

Despite being a long-awaited legislative development, the analysis concludes that the DPDPA is not sufficiently rights-protective due to design flaws and regulatory asymmetries. In order to align the Act with international best practices, constitutional principles, and the changing demands of India's digital society, the paper urges legislative reforms.

Reconfiguring Transparency: The DPDP Act's Impact on the Right to Information

The Digital Personal Data Protection Act, 2023, also known as the "DPDP Act," marks a turning point in India's data privacy laws. Although its goal is to ensure informational autonomy in the digital age, constitutional scholars, activists, and information commissioners

are all very concerned about its implications for democratic transparency, particularly with regard to the Right to Information Act, 2005 ("RTI Act"). The most notable change is that the DPDP Act removes the critical public interest override clause from Section 8(1) (j) of the RTI Act, which had permitted access to personal data when disclosure served a greater public interest.[1]

Prior to the amendment, "personal information" that was unrelated to any public activity or interest or that would result in an unjustified invasion of privacy was exempt from disclosure under Section 8(1)(j) of the RTI Act, unless the disclosure was justified by the greater public interest. This made it possible for information commissions to use a balancing test, which compares the public interest in transparency with the right to privacy of the individual. This interpretive balance has continuously been maintained by court rulings. The Supreme Court stressed in Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal that transparency must come first when public officials' actions or use of public funds are at issue.[2] Although privacy is important, the Court made it clear that it cannot be used as a cover for opacity in government agencies.[3]

However, this balancing mechanism is completely eliminated by Section 44(3) of the DPDP Act. Access to "personal information" is now unconditionally prohibited regardless of the public interest or the public function being carried out. Even in situations where openness is essential for democratic accountability, this shifts the legal presumption in favour of non-disclosure.

There has been notice of this change. Legal experts have cautioned that eliminating the public interest test would eliminate one of the most important instruments that citizens, activists, and journalists have to examine public authority.[4] For example, despite being essential to public discourse and confidence, access to information about the service histories of civil servants, disciplinary actions, or the educational backgrounds of elected officials may now be

[1] Right to Information Act, 2005, § 8(1)(j), amended by Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023 (India).
[2] Cent. Pub. Info. Officer, Supreme Court of India v. Subhash Chandra Agarwal, (2019) 11 SCC 1, 89–90.
[3] Id. at 90–91.
[4] Internet Freedom Foundation, *RTI Amendment via DPDP Bill: An Alarming Blow to Transparency*, https://internetfreedom.in/rti-amendment-via-dpdp-bill (last visited June 4, 2025).

prohibited.[5]

Furthermore, Section 2(13) of the DPDP Act defines "personal data" in a purposefully broad manner, including “any data about an individual who is identifiable by or in relation to such data”.[6] This definition's scope and ambiguity may include publicly funded scheme records, land ownership information, or even publicly available political candidate affidavits. These can now be denied under the pretence of protecting privacy if there is no public interest exception.

The democratic goal for which the RTI Act was passed could be undermined by this extension of privacy-based non-disclosure, which runs the risk of changing the RTI regime from a pro-disclosure norm to a privacy-dominated exception. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India notably acknowledged the coexistence of the rights to information and privacy and emphasised the necessity of proportionality and necessity in any restriction on either right.[7] These requirements are not met by the amendment, which leaves no room for independent review or contextual analysis.

According to scholars like Pratap Bhanu Mehta, the amendment's chilling effect on transparency results from an incorrectly absolute interpretation of privacy. He warns that in a nation that has long struggled against bureaucratic opaqueness, privacy without accountability mechanisms runs the risk of turning into the "instrument of authoritarian secrecy."

Given these events, the removal of the public interest override should be seen as a paradigm shift in the design of Indian democratic governance rather than a small legislative change. There could be serious repercussions, including diminished investigative journalism, a decline in public authority oversight, and a deterioration in public trust. Transparency cannot be sacrificed for unqualified privacy in a constitutional democracy. The public interest exception must be reinstated, adjudicatory discretion must be strengthened, and the twin objectives of accountability and privacy must be balanced in a statutory framework.

[5] See generally *Kush Kalra v. Union of India*, (2021) 11 SCC 517 (requiring the disclosure of judges’ appointments in public interest).
[6] Digital Personal Data Protection Act, No. 22, § 2(13), Acts of Parliament, 2023 (India).
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 125.

Excessive Central Government Control over the Data Protection Board: A Threat to Regulatory Independence

An independent and unbiased regulatory body that can enforce compliance, decide violations, and foster public trust is essential to any successful data protection regime. However, the Data Protection Board of India ("DPB") is established by the Digital Personal Data Protection Act, 2023 ("DPDP Act") in a way that compromises its structural and functional independence, giving rise to grave concerns about regulatory capture, conflict of interest, and the weakening of the rule of law.

Section 18 of the Act established the DPB, which is charged with deciding violations, enforcing sanctions, and guaranteeing adherence. Although this is similar to how international frameworks such as the General Data Protection Regulation ("GDPR") of the European Union empower independent supervisory authorities,[8] the Indian model falls short in both composition and oversight mechanisms.

The most obvious is that the Central Government still has broad control over how the DPB operates: The Chairperson and Board Members are chosen and dismissed at the Central Government's sole discretion, with no room for legislative or judicial review.[9]

Qualifications, terms of service, pay, and appointment conditions are also set by the government.[10] Instead of being a separate statutory authority, the Board is only categorised as a "adjudicating body.[11]

Additionally, the DPDP Act erodes confidence in the application of data protection standards by centralising authority, particularly when it comes to situations involving government data fiduciaries. For example, if the enforcement body is chosen, led, and removed by the State itself, and the State is one of the parties accused of misusing personal data, then the perception of bias is unavoidable.[12]

[8] Regulation 2016/679 of the European Parliament and of the Council, art. 51(1), 2016 O.J. (L 119) 1 [hereinafter GDPR].
[9] DPDP Act, § 19(1).
[10] Id. § 19(2).
[11] Id. § 18(2).
[12] Vrinda Bhandari & Renuka Sane, The Toothless Board in the Data Protection Bill, THE LEAFLET (Aug. 11, 2023), https://theleaflet.in/the-toothless-board-in-the-data-protection-bill.

In contrast, supervisory authorities are required by the European GDPR to "act with complete independence in performing their tasks."[13] Independent commissions or boards that are answerable to Parliament or the judiciary rather than the executive branch have been adopted by data protection regimes in nations like South Africa, Brazil, and Kenya.[14]

This executive-heavy model has drawn harsh criticism from Indian academics and civil society. Because DPB lacks independent selection committees, public reporting requirements, and appealable procedures outside of the Central Government's own ecosystem, it runs the risk of turning into a "toothless body without autonomy or public credibility".[15]

Additionally, this overbearing control runs counter to the rulings in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court stressed the importance of fairness, proportionality, and due process in governing data protection frameworks, especially given the State's extensive informational power.[16] These assurances become, at most, aspirational in the absence of an impartial regulator.

All things considered, the Data Protection Board's creation under the DPDP Act falls short of the level of independence necessary for a data protection system that upholds human rights. The Board's ability to enforce privacy rights against influential State or corporate entities will be called into question if its institutional design is not changed to include independent appointments, operational autonomy, and parliamentary oversight.

The Overbroad Scope of Section 7(b): State Processing Without Consent and Lack of Safeguards

Although this clause is framed in terms of "legitimate uses," its ambiguous wording, broad application, and abuse potential make it extremely risky from a legal and constitutional standpoint.[17] Although this clause is framed in terms of "legitimate uses," its ambiguous

[13] GDPR, art. 52(1).
[14] Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, 168 PRIVACY LAWS & BUS. INT'L REP. 10, 13 (2021).
[15] Internet Freedom Foundation, *Clause-by-Clause Analysis of the DPDP Act*, https://internetfreedom.in/iff-analysis-dpdp-2023 (last visited June 1, 2025).
[16] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 125.
[17] Digital Personal Data Protection Act, No. 22, § 7(b), Acts of Parliament, 2023 (India).

wording, broad application, and abuse potential make it extremely risky from a legal and constitutional standpoint.

As long as the data: Was previously consented to (clause i) or exists in any digitised or non-digitized official database notified by the Central Government (clause ii)[18], the provision permits government agencies to process personal data for the purpose of providing "subsidy, benefit, service, certificate, licence, or permit" without express consent.

This results in a significant departure from the Act's consent-centric structure. In particular, clause (ii) permits ex post facto regularisation of processing personal data by simply digitising old records and issuing a government notification.

In contrast to the EU's General Data Protection Regulation (GDPR), which permits such processing only under explicit safeguards[19] and on strict legal grounds (such as public interest or legal obligation), the DPDP Act's Section 7(b)(ii) does not impose such proportionality or necessity requirements. It is incompatible with contemporary privacy law since it permits data processing without the subject's knowledge or ability to object.

This subsections does not call for individual notice, transparency procedures, or even independent prior review. Because of the executive's unrestricted discretion granted by the phrase "notified by the Central Government," any database may be included in this exception. This gives the State the sole authority to approve any data processing.

The Supreme Court ruled in Justice K.S. Puttaswamy (Retd.) v. Union of India that any invasion of privacy must pass a four-part test of legality, necessity, proportionality, and procedural safeguards. This model runs counter to the principles established in that case.[20]

Function creep, in which data gathered for one purpose is used for another, could be made possible by Section 7(b). [21] For instance, without new consent, health information gathered for the purpose of issuing a medical certificate may subsequently be used for profiling or unrelated surveillance programs.

---

[18] Id.
[19] GDPR, art. 6(1)(e), Regulation 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.
[20] Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 165.*
[21]Usha Ramanathan, *A Blow to the Right to Privacy*, THE HINDU (Aug. 11, 2023), https://www.thehindu.com/opinion/lead/a-blow-to-the-right-to-privacy/article67175622.ece.

Furthermore, by allowing the government to digitise and notify any "book or document," the provision makes it possible to retroactively legitimise data collection from the past, even from situations where the data was initially provided under duress or involuntarily (such as caste surveys, police registers, or ration card enrolments).

Section 8(6): Absence of Timeline for Breach Notification Undermines Timely Remedies

Data Fiduciaries are required by law to notify the Data Protection Board of India and each impacted Data Principal in the event of a personal data breach, according to Section 8(6) of the Digital Personal Data Protection Act, 2023 (DPDPA).[22] However, there is no deadline for when this notification must take place; the section only specifies that it must be given "in such form and manner as may be prescribed.[23] There are serious practical and legal issues with this omission.

Section 8(6) is procedurally ambiguous and susceptible to Data Fiduciaries' delayed compliance because it lacks a clear deadline, such as 24, 48, or 72 hours. In actuality, this means that if a business eventually complies with the regulations after they are established, it may postpone notifying the Board or impacted users for days, weeks, or even longer without technically breaking the law. One of the main goals of breach notification minimizing harm through rapid action, is undermined by such regulatory silence, which permits risk concealment.

On the other hand, unless the breach is unlikely to put people at risk, a data controller is required by Article 33 of the General Data Protection Regulation (GDPR) of the European Union to notify the supervisory authority of a breach involving personal data within 72 hours of learning about it. This stringent timeline guarantees early warning and prompt response for affected parties and regulators.

In order for the Data Principal to exercise her rights under the DPDPA, including redressal, complaint filing, and corrective actions like password changes or account blocking, timely breach notification is essential. In situations involving health, biometric, or financial data, a

[22] Digital Personal Data Protection Act, No. 22, § 8(6), Acts of Parliament, 2023 (India).
[23] Id.

delayed notice may result in monetary loss, identity theft, or psychological distress.[24]

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court emphasised that maintaining one's privacy means having meaningful control over one's personal information, including the right to know when it is being misused.[25] This right becomes illusory in breach situations if there is no deadline for notification.

Section 8(6) over-relies on delegated legislation by leaving the entire breach notification procedure including its timeline to future regulations. In the interim, this weakens the statute's enforceability and compromises legal certainty. The absence of a clear statutory deadline permits regulatory evasion and weakens accountability, especially in light of the growing number and severity of data breaches in India.[26]

Removal of "Sensitive Personal Data" from the Final Act: A Dilution of Risk-Based Protections

The elimination of the "Sensitive Personal Data" (SPD) classification is one of the most notable changes made in the 2019 Personal Data Protection Bill by the Digital Personal Data Protection Act, 2023 (DPDPA). This modification marks a departure from the risk-based approach to data protection that the majority of contemporary privacy laws, such as the General Data Protection Regulation (GDPR) of the EU, have adopted.

Financial information, health information, official identifiers (such as Aadhaar), biometric and genetic information, caste or religious belief, sexual orientation, and more[27] were all explicitly defined as "sensitive personal data" in the Personal Data Protection Bill, 2019, which was primarily based on the Justice B.N. Srikrishna Committee's recommendations.

Along with additional safeguards like requiring storage in India for specific categories and prior approval for cross-border transfers, the 2019 Bill required explicit consent for processing SPD.[28] These safeguards acknowledged that improper use of such information could lead to

[24] Vrinda Bhandari & Renuka Sane, Data Breaches and the Case for Mandatory Reporting, THE LEAFLET (Aug. 12, 2023), https://theleaflet.in/data-breaches-and-mandatory-reporting.
[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 166.
[26] The Economic Times, *India Sees 700% Surge in Data Breaches in 2023*, https://economictimes.indiatimes.com (last visited June 1, 2025).
[27] Personal Data Protection Bill, No. 373, § 3(36), Lok Sabha (India), 2019.
[28] Id. §§ 11, 33–34.

serious negative effects like identity theft, stigmatisation, discrimination, or government monitoring.

The DPDP Act, 2023, on the other hand, defines "personal data" as "any data about an individual who is identifiable by or in relation to such data."[29] It treats all data equally, regardless of its nature, context, or potential for harm, because it does not distinguish between sensitive and non-sensitive data.

This is problematic for a number of reasons:

The act disregards the harm principle, which states that not all data is equally dangerous. Compared to, say, email preferences, financial or health data is intrinsically more vulnerable. The Act disregards the proportionality principle, which is essential to any framework based on rights, by failing to make a distinction between them.

It also compromises user autonomy: Users who agreed to the use of sensitive data were given more protections under the 2019 draft. Under a general consent mechanism in the 2023 Act, users may unintentionally consent to risky data uses.[30]

Reduces anti-discrimination protections: Without the SPD category, information about caste, religion, or sexual orientation may now be processed without stricter protections, raising the possibility of social exclusion and profiling, particularly in the hiring or welfare delivery processes.[31]

Most global data protection laws classify and treat sensitive data differently:

Sensitive data is classified and handled differently by the majority of international data protection laws: Under Article 9, GDPR acknowledges "special categories of personal data" and forbids processing them, with a few protected exceptions.[32]

[29] Digital Personal Data Protection Act, No. 22, § 2(13), Acts of Parliament, 2023 (India).
[30] Udbhav Tiwari, *India's Final Data Protection Law Disappoints on Rights and Accountability*, MOZILLA FOUNDATION (Aug. 14, 2023), https://foundation.mozilla.org.
[31] Renuka Sane & Vrinda Bhandari, The Problem With India's New Privacy Law, THE LEAFLET (Aug. 15, 2023), https://theleaflet.in.
[32] GDPR, art. 9, Regulation 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.

India's decision to remove this category is regressive, potentially rendering it in violation of international data transfer adequacy standards and endangering cross-border data collaborations with countries that have ratified the GDPR.

Removing SPD, according to some commentators, makes the law more "business-friendly" and streamlines compliance.[33] However, user vulnerability shouldn't be sacrificed for compliance ease. The goal of the data protection law is to empower people, not just lessen the burden of regulations.

Informational privacy is an aspect of dignity, as Justice Puttaswamy stressed, and treating sensitive data like any other compromises the constitutional guarantee of equal protection and individual liberty.[34]

Problems with Section 17 of the DPDPA: Broad Exemptions, Weak Oversight, and Risk of Executive Overreach

A number of privacy rights and obligations for safeguarding personal data are outlined in the Digital Personal Data Protection Act, 2023 (DPDPA). Nevertheless, the Act's "Exemptions" Section 17 establishes broad exceptions that permit the State and private organisations to handle personal data without abiding by the fundamental safeguards outlined in Chapters II and III of the Act.[35] These exclusions apply to everything from government operations, research, and corporate reorganisations to criminal investigations and lawsuits.

Many of the provisions in Section 17 are too general, ambiguous, or procedurally weak, which compromises the Act's overall integrity even though some exemptions might be required for operational flexibility. According to Section 17(1)(c), processing personal data "in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law" will not be subject to the Act's fundamental protections. [36] Despite having a valid goal, this exception has issues with its scope and design.

[33] Nikhil Narendran, A Business-Friendly Law That Misses the Privacy Bus, BLOOMBERGQUINT (Aug. 10, 2023), https://www.bqprime.com.
[34] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 122–23.
[35] Digital Personal Data Protection Act, No. 22, § 17, Acts of Parliament, 2023 (India).
[36] Id. § 17(1)(c).

Unlike the privacy doctrine established by the Supreme Court in Puttaswamy, the phrase "in the interest of" is too ambiguous and does not require necessity or proportionality.[37] Additionally, there is no independent or judicial oversight to determine whether this exception is being properly invoked. The GDPR, on the other hand, only allows these exceptions under certain conditions, including transparency, oversight, and protection of rights.[38]

As written, this section increases the possibility of abuse against journalists, activists, and marginalised communities by enabling government agencies to justify any type of data processing, including profiling and mass surveillance, without any oversight.

The Central Government may exempt any of its instrumentalities from the full Act under Section 17(2)(a) if doing so is "in the interests of sovereignty, integrity of India, security of the State..." and for other comparable grounds.[39]

Although international law recognises national security as an exception, the DPDPA:

- Does not require proportionality or necessity;
- Does not require publication or explanation of the exemption;
- Lacks judicial or independent review;
- Permits a broad exemption without any restrictions on time or subject matter.

This violates international norms as well as the privacy doctrine of the constitution. Such exemptions should be "narrow, necessary, and proportionate," according to the Justice Srikrishna Committee's recommendation, and they should be subject to "independent oversight."[40] The final Act disregarded these suggestions.

When processing is required to uphold a legal right or claim, subsection 17(1)(a) permits it, and when courts, tribunals, and regulatory agencies act in a judicial or quasi-judicial capacity, subsection 17(1)(b) exempts them.[41] Even though these exemptions seem reasonable, they are

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, 166.
[38] GDPR, art. 23, Regulation 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.
[39] DPDP Act, § 17(2)(a).
[40] Justice B.N. Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, MEITY (July 2018), https://www.meity.gov.in.
[41] DPDP Act, § 17(1)(a)–(b).

vague and unclear in their procedure, particularly when quasi-judicial functions are involved. Without strong safeguards, they could be used by a variety of entities, such as administrative regulators and tribunals.

Subsections 17(1)(d) to (f) exempt processing for debt recovery, mergers and corporate arrangements, and cross-border contracts.[42] These carve-outs are concerning because: The Data Principal need not be notified; even in cases involving substantial amounts of personal data, the exemptions are applicable.

It is not necessary to evaluate proportionality or grant a right to correction in the case of defaulting borrowers. Financially vulnerable people may be disproportionately impacted by financial profiling that lacks transparency and recourse.

The Central Government may exempt new businesses or groups of data fiduciaries from important rules like notice requirements, data minimisation, and purpose limitation under Section 17(3).[43] This weakens the law's protective scope by introducing regulatory arbitrariness and possibly encouraging companies to misclassify themselves in order to avoid compliance.

The Central Government may, for a maximum of five years, suspend the application of any Act provision to any class of data fiduciaries, as permitted by Section 17(5).[44] This broad and arbitrary authority jeopardize the legal system's stability and breeds doubt in the minds of fiduciaries and users alike.

Data Principals (i.e., users) are not granted notice, an objectional right, or an effective remedy under any of the aforementioned exemptions. Additionally, there are no independent oversight mechanisms, mandatory disclosures, or requirements for periodic review.

This stands in stark contrast to Puttaswamy, where the Court ruled that even legitimate State interests must be pursued through laws that are reasonable, fair, and just while also providing procedural safeguards.[45] The democratic and constitutional basis of India's privacy rights is in

[42] Id. § 17(1)(d)–(f).
[43] Id. § 17(3).
[44] Id. § 17(5).
[45] Puttaswamy, supra note 44, at 166–67.

danger of being undermined by Section 17, which could turn into a legal loophole for unrestricted surveillance, profiling, and arbitrary data processing

Section 37 and the Expansion of Executive Control: A Challenge to the DPDP Act's Transparency Goals

The goal of the Digital Personal Data Protection Act, 2023, is to safeguard people's privacy by regulating the processing of personal data by Data Fiduciaries, or organisations that decide how and why data is processed. However, there are significant problems with Section 37 of the Act because it is so broad and discretionary.

The inclusion of Section 37 of the Digital Personal Data Protection Act, 2023 (DPDPA) has sparked a number of legal and constitutional issues, despite the fact that it is intended to be an enforcement tool against repeat offenders of data protection standards. According to the section, if a Data Fiduciary has been penalised twice or more, the Central Government may, on the Data Protection Board's recommendation, block access to the data fiduciary's digital platform. But upon closer inspection, it becomes clear that the clause introduces serious constitutional and regulatory issues in addition to deviating from the fundamental goals of a data protection framework.

Protecting personal information is the main goal of data protection laws. However, because Section 37 concentrates on limiting access to information rather than addressing data misuse, it is similar to content regulation or censorship. Its inclusion in a privacy law seems out of place and runs the risk of confusing data protection with more general information control. A content blocking mechanism is already in place in India thanks to Section 69A of the IT Act of 2000. Without providing a clear rationale, Section 37 duplicates this authority, creating legal ambiguity and opening the door for misuse under the pretence of data protection.[46]

Conclusion and Suggestions

In order to control the processing of personal data and create accountability systems, the Digital Personal Data Protection Act, 2023 (DPDPA) is a significant piece of legislation in India's digital governance framework. This paper, however, shows that although the Act is a positive

[46] Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE INDIA (Aug. 2023), https://carnegie-production-assets.s3.amazonaws.com/static/files/Understanding_Indias_New_Data_Protection_Law-3.pdf.

step, it has serious structural and normative flaws that reduce its usefulness as a tool for protecting rights.

Important provisions in particular Sections 7, 9(4), 17, 20, and 37 give the executive excessive authority, permit broad exemptions without sufficient protections, and erode institutional autonomy. Transparency in democracy is further weakened by the elimination of the public interest override from the Right to Information framework. Concerns regarding fairness in procedure, legal certainty, and the suppression of digital innovation are also raised by the lack of set deadlines for enforcement actions and the possibility of preventing access to platforms without judicial supervision.

The DPDPA seems out of step with the requirements of legality, necessity, and proportionality when compared to international best practices like the EU's GDPR and constitutional principles, particularly those stated in Justice K.S. Puttaswamy (Retd.) v. Union of India. The following changes are suggested in order strengthen the legal framework and guarantee that the law protects both privacy and accountability:

1. Restore the Public Interest Override in the RTI Framework

Restore the public interest override under the Right to Information framework to guarantee that data privacy laws do not disproportionately restrict access to information, particularly in areas of public accountability, governance, and transparency. This would restore the necessary balance between the right to privacy and the right to information, as originally envisioned in Section 8(1)(j) of the Right to Information Act of 2005.

2. Ensure Independence of the Data Protection Board

Under Section 19 of the Digital Personal Data Protection Act, 2023, the Central Government has complete discretion over the appointment of the Chairperson and Members of the Board. This creates a risk of political bias and executive control.

Establish a multi-member selection committee comprising:

- The Chief Justice of India or a nominee (Chair),
- The Leader of the Opposition in Lok Sabha,

- The Cabinet Minister or Law Minister.

All appointments should be made through a transparent public notice and application procedure, followed by legislative vetting or independent oversight. Provide at least a 5-year fixed tenure. Removal should only be allowed on the basis of proved misbehaviour or incapacity, through a judicial process similar to that used to remove Election Commissioners or High Court judges.

The Board should submit annual reports to Parliament on complaints received, investigations conducted, penalties imposed, and compliance trends.

3. Limit Executive Blocking Powers Under Section 37

Introduce judicial review and proportionality checks before issuing blocking orders, and ensure that all such decisions are transparent.

4. Clarify and Codify Enforcement Timelines

Specify timelines for breach notifications (Section 8(6)) and complaint adjudication to uphold procedural fairness and reduce regulatory uncertainty.

5. Introduce Parliamentary Oversight of Rule-Making

Ensure that all delegated legislation under the DPDPA is subject to public consultation and parliamentary scrutiny to enhance transparency and prevent executive overreach.

In conclusion, while the DPDPA establishes the groundwork for personal data regulation in India, it needs to be significantly rebuilt to accord with constitutional values and international norms. A strong and balanced data protection system must empower individuals while constraining discretionary power and maintaining both informational privacy and democratic accountability.