

LAWFOYER INTERNATIONAL
JOURNAL OF DOCTRINAL LEGAL
RESEARCH
(ISSN: 2583-7753)

Volume 1 | Issue 4

2024

© 2024 *LawFoyer International Journal of Doctrinal Legal Research*

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of **any suggestions or complaints**, kindly contact info.lijdlr@gmail.com

To submit your Manuscript for Publication in the **LawFoyer International Journal of Doctrinal Legal Research**, To submit your Manuscript [Click here](#)

NAVIGATING THE PERSONAL DATA CONTOURS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Amri Gupta¹

I. ABSTRACT

The Digital Personal Data Protection Act, 2023, is a pivotal legislation in India's digital governance landscape, aiming to address the growing need for robust data protection laws in the digital era. It defines and regulates personal data, introducing key entities like Data Fiduciary and Significant Data Fiduciary, along with strict obligations and penalties for non-compliance.

However, the Act's impact is not without challenges, particularly in its potential conflicts with the Right to Information Act, 2005. Amendments to the RTI Act's Section 8(1)(j), expanding non-disclosure of personal data-related information, raise questions about the balance between data protection and the fundamental right to information. The role of the Data Protection Board emerges as crucial, tasked with providing clarity and guidance on the Act's implementation.

This article underscores the importance of striking a balance between data protection and the right to information, calling for nuanced approaches that safeguard privacy while ensuring transparency and accountability. It examines the Act's provisions and highlights challenges, emphasizing the vital role of the Data Protection Board in providing much-needed clarity. The analysis stresses the need for clear guidelines and robust regulatory oversight to ensure the Act's effective implementation.

While the DPDP Act 2023 is a significant stride in data governance, the importance of well-defined guidelines becomes evident as India adapts to the intricacies of the digital age.

¹ Student at *ICFAI Law School, IFHE, Hyderabad.*

II. KEYWORDS

Data Fiduciary, DPDP Act 2023, Personal Data, Processing, Rights

III. INTRODUCTION

In 2017, the privacy judgement² highlighted the need for digital data privacy. This stimulated the constitution of Justice BN Krishna Committee³ ("**Expert Committee**") under the MeitY⁴ to draft the first bill, i.e., the Personal Data Protection Bill, 2018⁵ ("**Bill 2018**"). After a series of consultations, the Bill was introduced within the Lok Sabha as the Personal Data Protection Bill, 2019⁶ ("**Bill 2019**"). The Bill 2019 then went through a thorough review by the Joint Committee of both houses of the Parliament ("**JCP**").

Owing to the advent of the COVID-19 pandemic, the anticipated date of JCP's report⁷ experienced a postponement, extending it to December 2021. This delayed report introduced a nascent legislative proposal denominated the Data Protection Bill, 2021⁸ ("**DP 2021**"). Nevertheless, given that 81 significant alterations have transpired since the JCP's report, the 2019 Bill was withdrawn. Then, in 2022, MeitY published a legislative note on the Digital Personal Data Protection Bill, 2022.

On 11th August 2023, the President assented to the Digital Personal Data Protection Bill, 2023 ("**DPDP Bill 2023**"), and now the Digital Personal Data Protection Act, 2023 (called the "**DPDP Act 2023**" or "**the Act**"). The Act went through the deliberations of the Houses of Parliament and was passed amidst protests, marking a significant

² K.S.Puttaswamy v. Union of India, (2019) 1 SCC 1.

³ A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, (2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

⁴ Ministry of Electronics and Information Technology, Government of India.

⁵ Personal Data Protection Bill, (2018),

https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

⁶ THE PERSONAL DATA PROTECTION BILL, 2019 - 164.100.47.4, (2019),

http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

⁷ Report of the Joint Committee on The Personal Data Protection Bill, 2019 (17th Lok Sabha), (2021),

https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

⁸ THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022 CHAPTER 1: PRELIMINARY, (2022), <https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>

milestone for India as it moves towards enacting its inaugural law governing the usage and processing of citizens' data by private or government entities.

The Act complements the previously scattered Indian data protection scheme ("**Old DPS**"), i.e., the Information Technology Act, 2000 ("**IT Act**") and associated rules⁹. It regulates the processing of digital personal data to recognise the rights of individuals by keeping intact the Indian legal provisions under one consolidated law.

IV. A SHIFT IN THE LEGAL FRAMEWORK

As we move towards a digital economy, using personal data has become very common in both public and private settings. Data's inherent value is enhanced when shared, resulting in significant efficiency gains. Nowadays, almost everything we do online involves some kind of data exchange, underscoring the significance of its regulation.

Previously, there was no specific law that protected the sharing or receiving of personal information, whether it's communicated verbally, in writing, or electronically. Nevertheless, the IT Act (Section 43A, 66 and 72A), coupled with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 ("**SPDI Rules 2011**"), governed the management of electronically exchanged data exclusively.

But, these regulations were inadequate in addressing the evolving digital landscape, which gave rise to the need for separate legislation that governs the protection of personal data in cyberspace. The arrival of the DPDP Act in 2023 is a game-changer for data protection. This law aims to find the right mix between respecting people's privacy rights and ensuring that personal data can be used effectively. While the Act holds considerable potential, further deliberation is necessary to provide clarity and resolution for any lingering uncertainties.

⁹ Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

This segment delves into critical facets of the DPDP Act of 2023, focusing on its provisions concerning the management of personal data. Within this section, we will identify potential limitations and propose remedial actions for consideration.

1. Defining 'Personal Data'

The IT Act didn't provide an exact definition of 'personal data,' ("PD") but it enforced a penalty (Section 43A) on companies if they fail to safeguard sensitive personal data or information ("SPD"). To substantiate, the SPDI Rules 2011 offered an inclusive explanation of what qualifies as 'sensitive personal data or information' in Rule 3.

The statutory definition of 'personal data' (Section 2(13) of the DPDP Act 2023) is broader than what was in the Old DPS. It now covers not only information about individuals (i.e. Personally Identifiable Information ("PII")) but also the results of automated actions and the idea of how easily a person can be identified from the information. This change is designed to be more comprehensive and accommodating.

Material Scope of Personal Data

The Act regulates how personal data is processed both within and beyond Indian territory. Where local applicability includes personal data that is either **digitally** collected or **converted to digital form**, overseas applicability only considers whether the Data Principal (the person with whom the personal data is concerned in relation to the offering of goods and services, and is referred as "DP") resides in India.

Exemption - Section 3(c)¹⁰ of the Act excludes the application of its provisions to the handling of personal data that is meant for personal or household use and has been made publicly available by the individual it belongs to, or as required by law. Moreover, the Act does not address the processing of data offline or the offline handling of data.

¹⁰ Digital Personal Data Protection Act, 2023, § 3(c), No.22, Acts of Parliament, 2023 (India).

2. Data Fiduciary and Significant Data Fiduciary

The Act assigns the responsibility of processing digital personal data to two key entities- the Data Fiduciary ("DF") and the Significant Data Fiduciary ("SDF"). While their core duties align, the SDF possesses specific additional authority.

Section 2(i)¹¹ defines a Data Fiduciary as the individual or entity empowered to decide both the purpose and the methods for processing personal data. A Significant Data Fiduciary, is a DF or a particular set of DF as determined by the Central Government, is chosen based on several key factors. These factors include – (a) the amount and sensitivity of personal data they handle; (b) the potential risk to the data subject's rights; (c) the impact on India's sovereignty and integrity; (d) implications for state security and public order; and (e) the potential impact on electoral democracy.

How is Data Fiduciary different from Data Processor? A Data Processor ("Processor") is an entity entrusted with the responsibility of managing personal data on behalf of a Data Fiduciary. When the Data Fiduciary holds the authority to define the purpose and methodology of data processing, the Data Processor's primary role centers around the processing of personal data. It's important to note that, unlike the Data Fiduciary, the DPDP Act 2023 does not contain a dedicated section outlining the distinct responsibilities of the Data Processor.

Point of Difference	Data Fiduciary	Data Processor
Authority Limitations	A DF can define the purpose and methodology of data processing.	A Processor's role is limited to what is instructed by a DF.
Consent & Notice Mandates	A DF requires consent of a DP for processing of personal data.	A Processor also requires consent of a DP for processing of personal data.

¹¹ Digital Personal Data Protection Act, 2023, § 2(i), No.22, Acts of Parliament, 2023 (India).

Obligations under the Act

- **Data Fiduciary** - The obligations¹² outlined in the Act closely mirror the core principles of the EU General Data Protection Regulation¹³ ("EU-GDPR"). To offer a concise summary of these requirements, they are as follows:
 - (a) Ensure compliance with the Act, regardless of whether data processing is carried out by the Data Processor or by itself, or if the Data Principal does not fulfil their obligations.
 - (b) Maintaining the *accuracy, completeness, and consistency of personal data* when making decisions that impact data principals or when sharing data with other data fiduciaries.
 - (c) Implementing effective *technical and organizational measures* to uphold the provisions of the Act.
 - (d) *Safeguarding personal data* in its possession or under its control by *taking reasonable security measures* to prevent data breaches.
 - (e) *Promptly notifying* the Board and affected data principals in the prescribed manner *in the event of a personal data breach*.
 - (f) *Making the contact information* of a *Data Protection Officer ("DPO")* or a designated representative *available* for data principals to inquire about their personal data processing.
 - (g) Ensuring *data deletion* when a data principal withdraws consent or when it is reasonably assumed that the specified purpose is no longer being served, while complying with applicable laws.
 - (h) Establish an effective mechanism to *address the grievances of data principals*.

¹² Digital Personal Data Protection Act, 2023, § 8, No.22, Acts of Parliament, 2023 (India).

¹³ European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016, Regulation 2016/679, European Union, 2016 (EU).

Section 8 aims to ensure that organizations who handle personal data must take certain steps to protect people's data rights. These steps involve *“implement appropriate technical and organizational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.”*¹⁴ This requirement extends to *“taking reasonable security safeguards to prevent personal data breach.”*¹⁵ However, the Act doesn't precisely spell out what counts as "appropriate" or "reasonable" in these measures. This is where the Data Protection Board's authority to make rules comes into play. They can provide more specific guidance on what qualifies as appropriate and reasonable safeguards to protect personal data.

- **Significant Data Fiduciary** - Section 11¹⁶ of the Act mandates SDF to fulfil following obligations:

- (a) *Appoint a Data Protection Officer ("DPO")* located in India. This individual shall serve as the official representative of the SDF, responsible for ensuring compliance with the provisions outlined in the Act. He is mandated to serve as an individual accountable to a board of directors or a similar governing body associated with the SDF. Additionally, the DPO assumes the crucial role of being the point of contact for addressing grievances.
- (b) Appoint an 'Independent Data Auditor' to assess the SDF's adherence to the Act.
- (c) Conduct the Data Protection Impact Assessment ("DPIA") and regular audits. A DPIA is a structured process that involves comprehensive data descriptions, clearly defined objectives, evaluations of potential harm, risk mitigation strategies, and adherence to specific requirements regarding the handling of personal data.

The execution of these obligations remains somewhat flexible, leaving room for Significant Data Fiduciaries to take autonomous measures in meeting their duties.

¹⁴ Digital Personal Data Protection Act, 2023, § 8(4), No.22, Acts of Parliament, 2023 (India).

¹⁵ Digital Personal Data Protection Act, 2023, § 8(5), No.22, Acts of Parliament, 2023 (India).

¹⁶ Digital Personal Data Protection Act, 2023, § 11, No.22, Acts of Parliament, 2023 (India).

This flexibility may introduce inconsistency and potentially harm the interests of Data Principals.

3. Processing of Personal Data

The Act requires organizations that handle data to ask individuals (called "**Data Principals**") *via* written notice for their "*free, specific, informed, unconditional and unambiguous*" consent.

The notice presented to the **DPs** must: (a) be in a clear, plain and unambiguous manner; (b) be in English or in any vernacular language (as per the requirement of DP and Eighth Schedule¹⁷);(c) be conspicuously available to the **DPs** during the procurement of consent and prior to the commencement of personal data processing; and; (d) consist of information of the intended PD and the underlying rationale of its processing, along with a delineation of **DPs** can exercise their rights under the Act (including the right to withdrawal of consent), and the remedy seeking measures through grievance redressal mechanism (under the Act). For instance—when opening a bank account through a bank's mobile app or website, a customer can choose a live, video-based customer identification process to meet Know-Your-Customer requirements. The bank must inform customers about the personal data being collected and its purpose before or alongside the request for data.

Consider another scenario where a social media app introduces a new feature for sharing users' locations with friends. Before a user, **B**, can use this feature, the app must inform **B** that by enabling it, their exact location (like GPS coordinates) will be collected and used to display on the platform. This notice is crucial as it ensures that **B** understands what they're agreeing to before deciding to share their location. Without this notice, the app cannot obtain valid consent from **B** to process their location data for the new feature.

¹⁷ INDIA CONST.sch.8, amended by The Constitution (Ninety-Second Amendment) Act, 2003.

Functional Constraints:

- (a) The DPDP Act 2023 provides an example: If a person downloads a telemedicine app and consents to the processing of their personal data for telemedicine services but is also asked for access to their contact list, they should only consent to the telemedicine purpose. This implies that DFs must justify specific data processing purposes. Some datasets, like location data, may be hard to justify unless they're directly related to the service, like map or delivery services.
- (b) Ensuring compliance with notice requirements can pose challenges for certain entities, particularly online platforms that exclusively operate in the English language. It is imperative that platforms are obligated to seek consent exclusively in the languages they actively support.

Furthermore, this mandate of seeking consent is *waived* by citing "*legitimate uses*" (Section 7), which include—(a) instances where a DP has willingly shared their personal data with the Data Fiduciary for a mutually agreed-upon purpose¹⁸; (b) situations where the State or its entities require the data to provide benefits to the Data Principal¹⁹; (c) cases in which the personal data is deemed crucial for the State's security, sovereignty, and integrity²⁰; (d) to comply with any legal obligation²¹; (e) occurrences related to medical emergencies²² and matters related to employment²³.

Evidently, the nuanced purview of the expression "*legitimate uses*" provides a shield to State entities, absolving them of liability towards the populace through reference to the interests of the State.

4. Rights of Data Principal vis-à-vis Duties of Data Fiduciary

Data Principals possess four main rights under the law. *Firstly*, they have the right to know what personal data is being shared with Data Fiduciaries and their ancillaries.

¹⁸ Digital Personal Data Protection Act, 2023, § 7(a), No.22, Acts of Parliament, 2023 (India).

¹⁹ Digital Personal Data Protection Act, 2023, § 7(b), No.22, Acts of Parliament, 2023 (India).

²⁰ Digital Personal Data Protection Act, 2023, § 7(c), No.22, Acts of Parliament, 2023 (India).

²¹ Digital Personal Data Protection Act, 2023, § 7(d), No.22, Acts of Parliament, 2023 (India).

²² Digital Personal Data Protection Act, 2023, § 7(f), No.22, Acts of Parliament, 2023 (India).

²³ Digital Personal Data Protection Act, 2023, § 7(i), No.22, Acts of Parliament, 2023 (India).

Secondly, they can correct or delete their personal data. *Thirdly*, they can designate someone to wield their rights if they become incapacitated. If any of these rights are violated by Data Fiduciaries or their affiliates²⁴ without 'valid legal grounds' (Section 8(7)), the DPs can turn to the Data Protection Board ("**DPB**" or "**Board**") for grievance redressal. The Act also allows for the appointment of 'Consent Managers' who will be officially recognised by the DPB. These Consent Managers will serve as representatives for individuals when it comes to handling their consent preferences.

Nevertheless, there are challenges that could impact the implementation of data principal rights. The DPB may face resource constraints when dealing with a potentially large volume of complaints. Additionally, some cases involving data principal rights might be complex, requiring detailed investigation and analysis, which could strain the resources of the DPB. Managing data transfers across borders while complying with domestic and international regulations can also be challenging, especially if there are conflicting laws in different jurisdictions.

While the idea of granting four significant rights and introducing a medium between Data Principal and Data Fiduciary called Consent Manager holds potential, there is a need for greater clarity on how these rights will be put into practice and the specific role that Consent Managers will play in safeguarding the rights of data subjects.

5. Personal Data Breach

The DPDP Act of 2023 outlines *three* specific actions that qualify as personal data breaches– (i) unauthorised processing; (ii) accidental disclosure, acquisition, sharing, use, alteration, destruction; or (iii) loss of access to personal data²⁵. In comparison, Section 43 of the IT Act addresses a similar concept, but it primarily focuses on hacking in the context of computers, computer systems, or computer networks. The DPDP Act 2023, however, requires a more detailed and clear elaboration of what constitutes a breach in the context of personal data. This clarification is crucial to ensure that both individuals and organizations can effectively adhere to the law.

²⁴ Digital Personal Data Protection Act, 2023, § 2(k), No.22, Acts of Parliament, 2023 (India).

²⁵ Digital Personal Data Protection Act, 2023, § 2(u), No.22, Acts of Parliament, 2023 (India).

In the event of a breach, the data fiduciaries are obligated to communicate the breach to the affected DPs and the DPB²⁶, but the timeframe of such an intimation is left uncovered. Section 27²⁷ grants the Board the authority to investigate breaches upon notification by the Data Fiduciary, Data Principal, Consent Manager, or any intermediary, and subsequently impose penalties, however, the Act lacks clarity on whether both the Fiduciary and the Processor involved in the same personal data breach are required to separately report to the DPB and the affected DPs, or if they can opt for a unified reporting approach.

This ambiguity in the reporting process leaves room for interpretational differences and potential misuse, such as—Without clear guidelines, organizations may struggle to determine the appropriate course of action in the event of a breach, potentially leading to non-compliance and legal repercussions. Breach reporting inconsistencies can undermine data subjects' rights, affecting their right to timely information, trust in data handling practices, and protection of personal information. Hence, clear and unambiguous guidelines in this regard are essential to ensure effective data breach management and uphold the principles of data protection and privacy.

6. Data Transfers

The Act distinguishes between two types of data transfers—one occurring among data fiduciaries within India and another involving data fiduciaries situated outside of India's borders²⁸. In both scenarios, a valid contract is essential for the transfer process. However, when it comes to transfers beyond India, an additional step is necessary. The Central Government must issue a notification specifying the countries where such transfers are legally permissible. On the other hand, the EU-GDPR allows data transfer to countries that have implemented adequate measures to ensure data protection, as detailed in Articles 45 and 46²⁹ of the regulation.

²⁶ Digital Personal Data Protection Act, 2023, § 8(6), No.22, Acts of Parliament, 2023 (India).

²⁷ Digital Personal Data Protection Act, 2023, § 27, No.22, Acts of Parliament, 2023 (India).

²⁸ Digital Personal Data Protection Act, 2023, § 16, No.22, Acts of Parliament, 2023 (India).

²⁹ European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

Under Section 16(2) of the DPDP Act of 2023, it is essential to emphasize that this new legislation does not take precedence over the existing transfer restriction requirements set forth by individual sectoral laws and administrative regulations in India. This added layer of oversight ensures that data is handled responsibly and in accordance with the law when crossing international boundaries.

7. Processing Personal Data of Children & PWDs

Children's or PWDs³⁰ personal data processing is permitted under the Act only after obtaining the "*verifiable consent of the parent of such child*". Organisations are restricted from processing data that can have a detrimental impact on the well-being of a child³¹, and the practice of directing targeted advertisements specifically towards children is strictly prohibited³². These measures are in place to ensure the protection and privacy of children in the digital realm, creating a safer online environment for the youngest users. For example–In the context of an online gaming platform designed for a young user base, stringent measures are in place to ensure the protection of minors' privacy and well-being. These measures include obtaining verifiable consent from parents or legal guardians before processing any personal data, such as names or ages. The platform is mandated to secure such consent. Therefore, the privacy of children in the digital space can be secured to some extent.

8. Penalties

The Act imposes heavy monetary penalties on violation of law. Priorly, the Old DPS worked on imposing similar steep monetary penalties, however, to date, there have been only a few isolated cases in which breaches of the SPDI Rules 2011 have resulted in fines or compensation payments.

95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016, Art. 45 & 46, Regulation 2016/679, European Union, 2016 (EU).

³⁰ Persons with Disabilities

³¹ Digital Personal Data Protection Act, 2023, § 9(2), No.22, Acts of Parliament, 2023 (India).

³² Digital Personal Data Protection Act, 2023, § 9(3), No.22, Acts of Parliament, 2023 (India).

The penalty ranges from Rs. 10K to Rs. 2.50 Crore. When imposing a monetary fine under Section 33(1), the Data Protection Body (DPB) is required to take into account several factors:

- (a) The seriousness, extent, duration, and frequency of the breach;
- (b) The type and significance of the personal data that has been compromised;
- (c) Whether the affected individual has suffered any harm or losses;
- (d) Whether reasonable precautions were taken to prevent the harm from occurring;
- (e) Whether the fine imposed is proportionate to the breach and its potential impact on the responsible party.

The Act falls short in empowering individuals affected by data breaches to seek compensation from DFs, potentially deterring them from undertaking costly adjudication processes before the DPB. Steps such as clearly defining the rights of individuals to seek compensation for specific breaches and a framework for assessing harm caused by breaches, including emotional distress and financial losses would help to mitigate such deterrent effects. Steps such as clearly defining the rights of individuals to seek compensation for specific breaches and establishing a framework for assessing harm caused by breaches, including emotional distress and financial losses, would help to mitigate such deterrent effects.

To promote transparency and fairness, it is advisable for the Act to require the Board to publish detailed guidelines on how penalties are determined. Furthermore, the reasoned decisions of the Board should be made accessible to the public, ensuring a more open and accountable system.

V. GREY AREA - THE RIGHT TO INFORMATION

The Data Protection Board is eagerly awaited to furnish thorough guidelines on how individuals can effectively exercise their rights as Data Principals, address personal data breaches, and define the responsibilities of Data Fiduciaries, which might fill in

the gaps in the interpretation of the Act. However, there is growing concern that the Act as a whole may not align seamlessly with the Right to Information.

Will RTI be severely hampered?

Right to Information (“RTI”) is a fundamental right under Article 19(1)(a)³³ and a statutory right under RTI Act of 2005³⁴ (“RTI Act”). The RTI is revolutionary because it allows an ordinary citizen to peek behind the curtain of government operations. If you know about RTI, you can ask any government agency to spill the beans on what they're up to. And guess what? They have to spill those beans, usually within a month. If they don't, the person in charge could end up paying a fine. This power of RTI through which any government entity can be asked to furnish information is at loggerheads with the DPDP Act of 2023. While the law may appear to be aimed at protecting people's privacy and data rights on the surface, a deeper look reveals some worrying issues about how well it actually works, how clear it is, and what might happen when it's put into action.

Where does the trouble lie?

The Act (by Section 44(3)) amends **Section 8 (1)(j)** of the RTI Act. By substituting clause “*information which relates to personal information*” to the amended Section, it expands the scope of non-disclosure of information, thus, misuse of this addition is a matter of concern. Highlighting the threat posed by this retrograde amendment, even the National Campaign for Peoples’ Right to Information (NCPRI) raised concerns when the DPDP Bill 2023 was introduced in the Lok Sabha. However, it was pushed through and became part of the Act.

The amendment shields all personal data from disclosure, eliminating the current exceptions. Presently, in order to withhold personal data, one must substantiate at least one of the ensuing justifications—the information sought lacks any connection to public activities; or it lacks relevance to any matters of public interest; or its disclosure

³³ State of Uttar Pradesh v. Raj Narain, 1975 AIR 865.

³⁴ Right to Information Act, 2005, § 3, No.22, Acts of Parliament, 2005 (India).

would result in an unjustifiable intrusion into an individual's privacy, and the PIO³⁵ or the appellate authority is convinced that there exists no overriding public interest that warrants divulgence. The overarching exemption proposed is particularly concerning as it fails to restrict the non-disclosure exemption solely to sensitive personal data³⁶.

Justice A.P. Shah's 2012 report³⁷ on privacy made a suggestion that, "*The Privacy Act should clarify that publication of personal data ... in public interest, use of personal information for household purposes, and disclosure of information as required by the Right to Information Act should not constitute an infringement of Privacy.*"³⁸ Empowering individuals to collectively monitor and access their rights and entitlements hinges on having readily available, detailed data, including personal information. Therefore, the said amendment is not appreciated and, if not intervened, may result in the exploitation of powers.

VI. CONCLUSION

The DPDP Act of 2023 has garnered attention as a significant piece of legislation that could reshape data governance in today's digital world. While it shows promise, there is a need for greater clarity and elaboration. Without well-defined guidelines and rulings, can the Act effectively function in a watertight compartment when it comes to addressing the complexities of a rapidly evolving digital landscape in India? The DPDP Act of 2023 presents several gaps, as elucidated in the preceding subheads. These gaps necessitate the eagerly awaited creation of guidelines by the Data Protection Board. In the interim, the existing IT Act and associated regulations can serve as valuable supplements to the Act, extending crucial support and direction to both Data Principals and Data Fiduciaries as they navigate this novel data governance framework.

³⁵ Right to Information Act, 2005, § 8(2), No.22, Acts of Parliament, 2005 (India).

³⁶ Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 3, 2011 (India).

³⁷ *Report of the Group of Experts on Privacy*, Centre for Internet & Society (Sept. 1, 2023, 9:30 A.M.), <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>

³⁸ *Id.* at 18.