RES MILITARIS Social Science Journal

A Critical Analysis of the Contemporary Regulatory Measures Relating to Data Protection

Riddhi Tripathi, Sanjay Tripathi, Sadhana Trivedi,

Faculty of Juridical Sciences, Rama University, Kanpur, U.P, India

ABSTRACT

Today personal data has grown into a valuable of global economy, which is becoming progressively more data driven. Comprehensive data protection policies are more crucial than ever as people are committing increasingly more of their personal information to digital services and platforms. An extensive structure for the protection of personal data in India is the crucial intent behind the 2023 enactment of the Indian Digital Personal Data Protection Act (DPDPA). This paper aims to explain the legislative challenges, compliance requirements, and ethical issues surrounding the Data Protection Act (DPA) and the emerging field of Data Protection in India.

The author through this research paper aims to analyze these complex issues and provide insightful information about effective tactics that government and companies may use to successfully negotiate and evade the regulatory environment. Furthermore, to analyze that the establishment of the Personal Data Protection Authority (PDPA) has given rise to a fundamental institutional framework responsible for implementing data protection laws.

Maintaining data privacy requirements and building confidence depend heavily on the PDPA's essential role in monitoring privacy and making sure they are in line with the DPA. In order to achieve regulatory compliance and deployment, this article outlines emerging best practices based on a thorough synthesis of relevant case studies and literature. In order to reduce risks and protect individual rights, it emphasizes the necessity of openness, equity, and technological responsibility when it comes to preserving user data. In summary, this study undertakes how data protection laws are still developing globally, whereas the violations of such data privacy are on the rise, thus creating an inversely proportional relationship. It emphasizes how vital it is to have a unified legal framework that upholds data privacy requirements while also encouraging innovation and creating an environment that is favorable to the responsible development and the use of latest modern technologies.

Keywords: Data, Privacy, Data Privacy, Digital Personal Data Protection Act (DPDP), Data Protection Board (DPB).

1. INTRODUCTION

In the 21st-century world where technology has become the defining paradigm, India's ongoing Data Protection regulation highlights the country's commitment to establishing a robust data privacy framework. Developing effective privacy governance procedures is essential for creating a transparent,

long-lasting, and sustainable company in the future. It also reduces reputational and business risk.[1] The processing of digital personal data inside the borders of India, whether it is offline data gathered and then digitized, is subject to the Digital Personal Data Protection (DPDP) Act, 2023. If it entails offering products or services to the data principals inside India's borders, it also applies to the processing of digital personal data outside of that country.

The kind and volume of personal data that is gathered, stored, processed, retained, and disposed of in India means that the act is anticipated to have an effect on most organizational areas, including legal, IT, human resources, sales and marketing, procurement, finance, and information security. Therefore, businesses operating in these and similar industries need to create a robust data privacy and security implementation program relating to the same. [2]

2. THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023 (DPDP):

The Digital Personal Data Protection Act of 2023 is the governing name of the Digital Personal Data Protection Bill of 2022, which was approved by each house of Parliament and promulgated into law by the president. Regardless of whether the data was initially gathered in a digital or non-digital format and then converted to a digital format, this Act, which came into force recently, controls the processing of digital personal data in India. [3] The government may choose to exclude state agencies from the DPDP Act's requirements.

The purpose of this law is to strengthen data protection and accountability for organizations that manage citizens' data, including mobile app developers, internet service providers, and corporations. It's also important to remember that the DPDP Act would affect India's trade talks with foreign countries. It follows international data protection regulations, drawing guidance from frameworks such as China's Personal Information Protection Law (PIPL) and the EU's General Data Protection Regulations (GDPR).[4]

This crucial piece of digital legislation was submitted during the ongoing Monsoon Session of Parliament, which began on July 20, 2023, and approved by the Union Cabinet on July 5. It moved quickly through the legislative process, being approved on August 7 by the Lok Sabha, the lower house, and August 9 by the Rajya Sabha, the upper house. The President's assent to the DPDP Bill, 2022, made it the officially the Digital Personal Data Protection Act on August 11, 2023.[5] The primary goal of the DPDP Act is to provide a greater degree of responsibility and oversight for enterprises that operate in India, such as mobile app developers, internet service providers, and corporations that gather, store, and handle personal

[1] L. Kalra, Decoding the Digital Personal Data Protection Act, 2023, *EY US.* (https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 visited10 January 2024).
[2] Ibid.
[3] 'A Comprehensive Guide to the India Data Privacy Law.' *India Digital* (https://secureprivacy.ai/blog/india-digital-personal-data-protection-act-2023-guide-protected-data) visited 16 February 2024
[4] K. Anand and M. Cyrill, 'India's Digital Personal Data Protection (DPDP) Act, 2023' *India Briefing News* (https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/) visited 12 January 2024

[5] 'India - Data Protection Overview' *Data Guidance* (https://www.dataguidance.com/notes/india-data-protection-overview visited 16 January 2024

data of Indian individuals. [6] This legislation prioritizes the privacy and data protection rights of Indian individuals by putting a significant focus on the "Right to Privacy" and making sure these institutions operate publicly and accountable while managing personal data.

The DPDP Act's reach goes beyond India's boundaries to include overseas digital personal data processing operations. This expansion mostly pertains to companies who profile and store Indian nationals while marketing products or services to people in India.

2.1 Key proposed changes in the digital legal infrastructure:

In order to address the governance of personal data in India, the DPDP Act currently serves as an essential component alongside the Proposed *Digital India Bill* and the proposed *Indian Telecommunication Bill, 2022.* When taken as a whole, these legislative initiatives mark a major advancement in supporting data privacy in the nation's rapidly changing digital environment. The Information Technology Act (IT Act) of 2000 will be superseded in India with the forthcoming Digital India Bill 2023. [7] By establishing thorough oversight over India's digital landscape, this new legislation aims to address a number of current issues, including cybercrime, data protection, deep fakes, platform competition, online safety, and the unfavorable effects of artificial intelligence.

The Indian Telegraph Act of 1885, the Indian Wireless Telegraphy Act of 1933, and the Telegraph Wires (Unlawful Possession) Act of 1950 are superseded by the Draft Bill *Indian Telecommunication Act, 2023*. Telecom network operation and service provision will require licenses. It sought to apply the licensing system that was previously in place for broadcasting services to internet communication services like Whats app, Signal, Google meet, Zoom, Skype and Gmail.[8] The democratization of internet communication services and the extension of monitoring and suspension capabilities from traditional broadcasting services would destroy user rights and democratic liberties beyond repair.

3. INTERNATIONAL DATA PROTECTION MODELS

3.1 The European Union (EU): The General Data Protection Regulation (GDPR)[9] of the EU places strict obligations on enterprises to guarantee that personal data is protected and requires proof of this. The rule gives consumers more control over how their data is used and safeguarded by establishing strict guidelines for gaining consent. The General Data Protection Regulation (GDPR), which is widely regarded as a groundbreaking and important legal framework, provides useful direction to nations in establishing the basic rights and obligations that should be incorporated into their respective data protection legislation. Its main goal is to successfully address the issues raised by our world becoming more digitally and networked.

3.2 The United States (US) model: The US model places a strong emphasis on preventing government interference into an individual's personal privacy. It allows for the gathering of personal data as long as

[6] V. Nayak, *Understanding the Right to Privacy* (https://cic.gov.in/sites/default/files/2012/R2Privacy-Venkatesh.pdf visited 12 January 2024

[7] T. Panjiar and P. Waghre, 'First Read: The Telecom Bill, 2023 Is on Santa's Evil List' *Internet Freedom Foundation* (https://internetfreedom.in/first-read-telecom-bill-2023/ visited 15 January 2024.

[8] 'The Telecommunications Bill, 2023' *PRS Legislative Research* (https://prsindia.org/billtrack/the-telecommunication-bill-2023 visited 12 January 2024

[9] Regulation (EU) 2016/679

the subject is informed about the data collecting process and its intended purpose. The United States of America, in contrast to several other nations, has a multitude of federal and state regulations that are intended to safeguard the personal information of its citizens.

Data Security Laws in America are primarily two mainly to be considered, Enhancement of Identity Theft Penalty Act (2004), Act to Prevent Identity Theft and Assumption. However, The Federal Trade Commission (FTC) is the principal enforcer of these laws in the U.S. In recent years, the FTC has taken several enforcement actions against companies that have misled consumers about their data security and privacy practices. U.S. Privacy Act, 1974[10] and a few other notable rights and restrictions under the mentions act on data held by government agencies are; Health Insurance Portability and Accountability Act (HIPAA),1996, dealing with healthcare and health insurance personal data protection. Gramm-Leach-Bliley Act (GLBA), 1999 it protects financial nonpublic personal information (NPI) and Children's Online Privacy Protection Act (COPPA) 2000, protects the personal information of those age 12 and younger.[11]

3.3 The China model: To prevent the unlawful use of personal data, China's Personal Information Protection Law (PIPL), 2021 grants data principals more rights than its counterparts. Important concepts covered by the legislation include processing, sensitive personal information, and personal information. Interestingly, it states clearly that it has jurisdiction over international borders. The Personal Information Protection Law (PIPL) encompasses essential components of data protection, such as guidelines for handling personal data, consent and non-consent-based processing reasons, cross-border data transfer procedures, and data holder's rights.

4. Overview/ Analysis of provisions India's Digital Personal Data Protection Act, 2023:

By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age. The DPDP Act, 2023 is a more moderate version of the law than the 2019 version data protection bill it includes less requirements for corporations and greater protections for consumers. The regulatory framework is less complicated, but it also gives the government certain unrestrained discretionary powers in particular situations. Key provisions of the DPDP Act, 2023 are as follows:

Consequence of Personal data breach: Any unlawful processing of personal data as well as unintentional disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that jeopardizes the data's availability, confidentiality, or integrity are all considered personal data breaches. The significant aspect of this Act is with regards to the consent for Processing of Personal Data. According to Section 6 of the Act, the Data Principal's (individuals who own the said data) consent must be free, explicit, informed, unconditional, clear, and accompanied by a definite affirmative action. It will only include Personal Data that is required for the intended uses. A noteworthy aspect of the Act is that,

[10] FP Pittman, A Hafiz and A Hamm, 'Data Protection Laws and Regulations Report 2023-2024 USA' *International Comparative Legal Guides International Business Reports* (https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa) visited 22 January 2024

[11] D Harrington, 'U.S. Privacy Laws: The Complete Guide' (https://www.varonis.com/blog/us-privacy-laws) visited 10 January 2024

in contrast to international norms of "Opt-in," Data Fiduciaries must get the approval of Data Principals and grant them an "opt-out" right.

Only with the individual's consent and for a reasonable or legal purpose may personal data be handled.[12] Prior to requesting consent, notification must be given. Information regarding the Personal Data that will be gathered and the reason for processing it should be included in the notification.[13] To make the said laws as unobtrusive as possible and facilitate the growth of commerce. When providing consent for the processing of their personal data, the data principal will have the choice to examine the notice and consent form in English or any other language listed in the Indian Constitution's Eighth Schedule. This will be beneficial to many people who do not speak English well. In cases where the data principal has consented to the processing of their personal data prior to the law going into effect, the data principal must receive a notice of this kind as soon as it is reasonably possible. As a result, in contrast to equivalents in other areas of the world, protection for previously granted permission has also been granted.

Application of the act: All data in India, whether initially offline and thereafter digitalized, is covered under the DPDP Act. Furthermore, the Act also covers the processing of digital personal data outside of India, especially where it involves providing products or services to people within of India. Businesses that gather information about Indian citizens are subject to the DPDP Act. It's interesting to note that non-citizens residing in India are also covered if their data is processed "in connection with any activity related to offering of goods or services" outside of India.[14] This has ramifications for situations where a supplier headquartered outside of India provides digital products or services to a U.S. citizen living in India.[15]

Individual permission to use data and principal rights related to data: The new law states that personal data can only be included and processed with the individual's express agreement, unless there are special circumstances involving national security, the law, or order. Individuals' rights to knowledge, deletion and correction of data, grievance redress, and the ability to designate another person to exercise these rights in the case of the individual's death or incapacity are all included in the data main rights. The introduction of data principle rights and grievance redress does not currently have a set schedule.

Purposes of Data Collection and Processing: The 2023 Act permits the processing of personal data for any legitimate reason. The party handling the data may do so with the agreement of the person being processed or for "legitimate uses," as defined by law. [16]

The following scenarios are considered legitimate uses: (a) when a person voluntarily provides personal data for a designated purpose; (b) when a person has previously given permission to receive any other kind of service from the state, such as a license, certificate, or permit; (this is a potential problem because it allows various government agencies that provide these services to access personal data that is stored

[12] The Digital Personal Data Protection Act, 2023 Section 4 & 6.
[13] Ibid. Section 5.
[14] Ibid. Section 3.
[15] A Burman, "Understanding India's New Data Protection Law" (*Carnegie India*, October 3, 2023) (https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624 visited February 11, 2024
[16] The Digital Personal Data Protection Act, 2023, Section 4.

with other government agencies);[17] (c) security or sovereignty; (d) meeting a legal requirement to provide information to the state; (e) adhering to rulings, decrees, or orders; (f) an emergency involving a medical crisis, a threat to life or public health, an epidemic, or a breakdown in public order.[18]

4.1 Obligations on Data Fiduciaries:

Data fiduciaries under the act are those organizations that are in charge of gathering, preserving, and handling digital personal data are subject to certain duties. The primary distinction between the 2019 bill and the 2023 act is the lack of authority for the regulator, the DPA, to establish comprehensive regulations on the wide categories of obligations given to the data fiduciaries. Furthermore, there have been reductions to the substantive criteria under each of these groups.

Significant data fiduciaries (SDFs) are another subset of data fiduciaries. Based on a number of factors, including the volume and sensitivity of data as well as threats to data protection rights, electoral democracy, security, and public order, the government will appoint data fiduciaries as SDFs.[19] Earlier SDFs were obliged to register in India under the 2019 bill. In the 2023 legislation, this need has been deleted.

4.2 The data protection board

The DPB is established under the 2023 statute.[20] The board differs greatly from the DPA and is not a regulatory body. In contrast to the latter, the board's authority to supervise data breach prevention, order corrective action, conduct investigations, and impose fines for legal noncompliance is more restricted. The board lacks the authority to establish rules or conduct codes or to request information in order to monitor how enterprises are run. It is limited to doing so when conducting inquiries.[21] The government will nominate board members, and regulations developed by the government will specify the terms and circumstances of their employment.[22]

4.3 Exemptions from Obligations under the Law

The majority of data fiduciary responsibilities, notification requirements, permission requirements, and associated requirements are exempted by the legislation for certain purposes and entities, as follows:

Processing in the purpose of maintaining public order, safeguarding the state's security, fostering cordial ties with other nations, upholding India's sovereignty and integrity, or avoiding incitement to any crime that may be prosecuted. This will enable security and investigative organizations to continue operating outside the boundaries set by this law.[23]

Processing of data is required for statistical analysis, research, or archiving where no decisions pertaining to a data principal are to be made using the personal data. Certain kinds of data fiduciaries, such as

[17] Ibid. Section 7(b).
[18] Ibid. Section 7.
[19] Ibid. Section 10.
[20] Ibid. Section 18.
[21] Ibid. Sections 27 and 28.
[22] Ibid. Sections 19 and 20.
[23] Ibid. Section 17(2).

startups, may be excluded from various requirements set out by the government, including certain key notification, completeness, correctness, consistency, and erasure of data by such business organizations. A concerning clause permits the government to declare that any provision of this legislation will not apply to any data fiduciary or classes of data fiduciaries for a time that may be stated in the notice, "before expiry of five years from the date of commencement of this Act."

This is a substantial and broad discretionary power that is unrestricted by any guidelines on the reasons for the exemption, the kinds of situations in which it can apply, or the duration of the exemptions.

4.4 A New Framework for Regulation of Data Privacy

The intended regulatory institutional framework earlier brought is entirely altered by the 2023 law. The bill from 2019 suggested creating a separate regulatory body. The DPA was modeled after comparable government organizations in many EU nations that carry out GDPR implementation and operate independently of the government. Since it was intended to have far more comprehensive regulation-making powers than DPAs under the GDPR, the planned Indian DPA was arguably more potent. Apart from formulating legislation, the DPA would have been tasked with creating corporate codes of conduct, looking into noncompliance instances, gathering supervisory data, and fining companies.

The government will nominate board members, and regulations developed by the government will specify the terms and circumstances of their employment. According to the legislation, throughout a member's tenure, these terms and conditions cannot be changed to their detriment under contrast; the DPB is established under the 2023 statute.[24]

The board differs greatly from the DPA and is not a regulatory body. In contrast to the latter, the board's authority to supervise data breach prevention, order corrective action, conduct investigations, and impose fines for legal noncompliance is more restricted.[25]

According to the statute, the board may fine parties up to 250 crore rupees, or around $30.5 million.[26] The Telecom Disputes Settlement and Appellate body is an established body that will hear appeals from the board's rulings (TDSAT). The measure permits data fiduciaries to offer voluntary undertakings to the board in exchange for any complaints being resolved against them, in addition to financial penalties.[27] As a result, in terms of architecture, the board differs greatly from the DPA. Lastly, a new clause that was not covered or included in any other edition of the legislation is incorporated in the 2023 version. This is Section 37, which gives the government the authority to prevent the public from accessing any material upon a board referral.

[24] Ibid. Section 18.
[25] Ibid. Sections 27, Section 28.
[26] Ibid. Schedule to the Act, Section 33.
[27] Ibid. Section 32

5. ANALYZING THE DPDP ACT, 2023

It begins by outlining the general framework of the legislation and highlighting its salient characteristics and problems. Secondly, it provides background information on the many versions that were previously submitted and expounds on the discussions that culminated in the creation of this statute.

5.1 The DPDP Act and protection of privacy:

India now has data privacy legislation for the first time thanks to the 2023 act. Prior to processing personal data, consent must be obtained, and the legislation explicitly lists a limited number of exceptions. Along with the right to nominate, it gives customers the ability to see, update, modify, and remove their data. It adds further security measures to the way children's data is processed. Businesses are then required to give notice of data gathering and have their purposes limited.

It imposes duties on organizations to provide notice of data collection and processing, limit its use, and provide security measures. Businesses are required by law to establish grievance redress processes. In addition, the DPB will manage grievances and complaints and has the authority to impose fines for breaking the law. India now has a regulatory framework for data protection for the first time. The existence of the legislation will eventually cause companies that gather data to progressively establish minimum standards of conduct and compliance.[28] The government's strategy for putting the legislation into effect and enforcing it will be crucial in this respect. For instance, it will be crucial to determine whether the law's implementation would target companies that rely heavily on data or the whole economy.[29]

Aside from unanswered implementation-related difficulties, there are certain worries about various legislation sections and their potential to undermine the safeguards that the law appears to provide. First, the exclusions made for consent give the state considerable power and elevate governmental requirements above those of private organizations.

Although there are situations in which this is absolutely justified, such as during crises or catastrophes, the legislation expands the range of these situations. For instance, the law permits the government to circumvent consent requirements in cases when a beneficiary of government services has already given permission to receive any other benefit from the state[30]. While this could make it simpler for the government to get recipients' personal information so they can receive services, it also raises the possibility that the government might misuse database, with fewer restrictions.

The collection of exemptions granted to the state for criminal prosecution, investigative, and national security purposes is another illustration of this. The legislation exempts notice and permission obligations, among others, for processing intended for "prevention, detection, investigation or prosecution of any

[28] Mihir R, 'Digital Personal Data Protection Act, 2023: A Missed Opportunity for Horizontal Equality', 'Digital Personal Data Protection Act, 2023: A Missed Opportunity for Horizontal Equality' (19 February 2023) visited 19 January 2024

[29] Dowden M, "India Welcomes Landmark Data Protection Law | Privacy World" (*Privacy World*, August 16, 2023) https://www.privacyworld.blog/2023/08/india-welcomes-landmark-data-protection-law/ visited 17 January 2024

[30] The Digital Personal Data Protection Act, 2023,Section 7(b)

offence or contravention of any law,"[31].This makes sense; however in the interests of public order, sovereignty, security, integrity, and avoiding provocation, Section 17(2) (a) thereafter grants any government agency that the government may notify a broad exemption from the whole statute. Section 17(2) (a) just expresses Parliament's intention to guarantee that the data privacy legislation is completely not applied to specific state agencies, as Section 17(1) (c) already exists.

These kinds of provisions establish a distinct category of activities that are not covered by data privacy regulations. The fact that the Indian state is exempt from many of the regulations that apply to private organizations is problematic, particularly when there is no urgent need for an exception of this kind. Second, the safeguards afforded by the law may occasionally be compromised by the government's arbitrary rule-making authority. For instance, within five years of the legislation's enactment, the government may proclaim, pursuant to Section 17(5), that no firm or class of enterprises would be subject to any of the requirements of this law. There is no timeline or guidelines for when this exception will be in effect about the use of this clause. If one were to read this clause optimistically, it may be utilized to give startups or emerging businesses more time to comply with the law.

Section 17(3), which grants limited exemptions to startups and other businesses the government may announce, has already established provisions for this. Consequently, there is a chance that Section 17(5) will be applied in a way that undermines the intent of the legislation. It is important to emphasize that the legislation only restricts the government's ability to provide certain exemptions for a five-year beginning term. There is no time restriction on the duration of these exemptions.[32]

Comparably, the government can exclude companies from various regulations governing the handling of children's data through the use of its arbitrary rule-making authority. Sections 9(1) through 9(3) outline specific standards for the same; among other things, they forbid profiling and demand parental approval. Any firm or class of enterprises may be excluded from Sections 9(1) through 9(3) by the government "subject to such conditions, as may be prescribed," according to Section 9(4). Once more, this clause is vague about the requirements that must be met, the basis for granting this exception, and other details. This clause can potentially be abused because there isn't enough instruction.[33]

Third, there are issues with the DPB's design. The government will establish procedures for the appointment and selection of the board's members. The board is an autonomous body with a restricted mandate. The statute specifies the requirements for members, but it does not specify the number of members that must be on the board or that one must be a legal expert. Given that one of the board's primary responsibilities is to impose sanctions and directives for noncompliance, this final clause is problematic. Furthermore, the DPB chairman has the authority to give any board member permission to carry out "any of the functions of the board and conduct any of its proceedings."[34]

Additionally, the internal division of duties between the chairman and the members conducting the inquiry is broken by this design. Since the chairperson designates members to undertake investigations,

[31] Ibid, Section 17(1)(c).
[32] Ibid. 5
[33] I.P. Massey, “Chapter 4” in Administrative Law, 10th ed. (Lucknow: Eastern Book Company, 2022), 94–104.
[34] [34] The Digital Personal Data Protection Act, 2023,Section 26(c).

they could not always carry out their duty impartially. Thus, even if the DPDP Act establishes legal protections for data privacy for the first time, if the government does not implement any of the law's requirements with the utmost rigor, its advantages may be substantially undermined.[35]

6. CRITICAL ANALYSIS OF THE DEVELOPMENT OF THE DPDP ACT:

In contrast to the 2018 draft law and the 2019 bill that was tabled in Parliament, the DPDP Act represents a significant change in the direction of data protection legislation. The November 2022 draft bill was where this change was most noticeable, and it is now a part of the 2023 legislation. This change is seen along three primary axes.

1. Declines in responsibilities and rights, as well as compliance: The bill's 2018 and 2019 iterations enacted a more comprehensive and expansive data protection structure. Many of these duties and privileges have been eliminated or have been reduced in scope. This is a more effective and innovative method. Businesses will experiment with various methods to incorporate data protection into business processes because there is currently no precedent for data protection legislation or jurisprudence. The DPB, the TDSAT, and the courts will provide decisions about practices that do not comply with the DPDP Act's standards.[36] Good practices that are appropriate for the Indian setting will naturally develop as a result of this approach.

It is important to consider the movement away from criminalization while evaluating the decrease in prescriptive requirements and overall compliance. The 2018 law added many new criminal charges. This was reduced to only one in the 2019 bill that is, deanonymization. The 2022 draft and the 2023 version solely specify monetary penalties to be imposed by the DPB, leaving out any mention of criminal violations.

2. A greater emphasis on data privacy: Several clauses in the 2018 and, more importantly, 2019 drafts contained information that was only loosely connected to data privacy. For instance, there was no way in which the clause requiring the disclosure of non personal data advanced privacy interests. Similarly, it has been demonstrated that data privacy and data localization requirements simply have a passing connection and better options are available to accomplish the same goals. There was some ambiguity over their inclusion in the legislation for 2018 and 2019. Furthermore, data localization evolved becomes a stand-in for discussions on topics like data sovereignty, which is once more unrelated to privacy concerns.[37]

3. The repeal of a "regulatory" statute: A highly regulated legislative framework was established by the 2018 and 2019 bills, which gave the DPA, a fully fledged independent regulator, broad authority to create regulations and codes of conduct on a number of their provisions, including notice and consent

[35] Report of the Joint Committee on the Personal Data Protection Bill, 2019," 17th Lok Sabha Secretariat,December 16, 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.
[36] Ibid. 26
[37] Balasubramanian A, "India: India's New Data Protection Law: Simply Put" (*Mondaq*, February 1, 2024) (https://www.mondaq.com/india/privacy-protection/1417428/indias-new-data-protection-law-simply-put visited February 10, 2024

requirements, security precautions, data storage practices, and more. [38] Furthermore, the DPA would have had the authority to gather the required.

4. Over-reliance on laws that have been sub delegated

Delegated law gives different administrative bodies a great deal of discretion, which might result in widespread misuse or the abuse of disproportionate power. The government has purposefully left this piece of law up to the whim of lower-level authorities under the guise of making it appropriate. Justice B.V. Nagarathna reminded us in his dissenting opinion in the Supreme Court's finding on demonetization that unrestrained and unbridled powers under delegation would be inherently arbitrary and suffer from the sin of unconstitutionality.[39] The Act's overuse of the term "as may be prescribed" raises questions about how explicit and unambiguous its provisions are.

Since the legislation does not go deeply into the details of execution, it is excessively delegated. The centerpiece of this DPDP Act appears to be the government's favorite slogan, "as may be prescribed." Within a 21-page Act including 44 parts, it has been used 28 times. To enable the government to make arbitrary judgments, the uncertainty has been preserved. If the expression "as may be prescribed" appears in the bulk of the provisions, then no law can be considered sound proof. Therefore, the executive branch of government is free to make the choice at its will, which undermines the functions of the legislature.

5. Penalties and compensation: One striking shortcoming is the lack of a clause allowing the Data Protection Board to compensate data principals who have been wronged. Although the Board has the authority to penalize data fiduciaries who violate the Act, penalties that are sent to the Consolidated Fund of India under section 34, it lacks the authority to compensate the Data Principals who have been wronged. This shortcoming makes it more difficult for the law to effectively compensate people for genuine harm they have experienced as a result of data breaches or privacy violations.[40] It's interesting to note that the Act penalizes Data Principals for breaking any of its rules, with fines reaching Rs 10,000.[41]

If data fiduciaries disregard the regulations, they attract penalty of up to INR 2.5 billion. These include fines of up to INR 2 billion for failing to notify the Data Protection Board and affected data principals in the event of a personal data breach; penalties of up to INR 2 billion for violating additional obligations related to children's data, attracting penalties of up to INR 1.5 billion for failing to comply with additional obligations of significant data fiduciary and penalties of up to INR 10,000 for breaching the duty towards data principals. [42]

---

[38] Ibid.
[39] Vivek Narayan Sharma v. Union of India, 2023 SCC OnLine SC 1, decided on 02.01.2023
[40] 'INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: HISTORY IN THE MAKING' (*Nishisht Desai*, 12 October 2023) (https://www.nishithdesai.com/NewsDetails/10703#:~:text=The%20Board%20will%20inquire%20into,costly%20adjudication%20before%20the%20Board. visited 16 January 2024
[41] 'Data Protection Bill May Cap the Maximum Penalty for Violations at Rs 250 Crore' (*The Hindu buisnessline*, 17 November 2023) (https://www.thehindubusinessline.com/info-tech/data-protection-bill-may-cap-the-maximum-penalty-for-violations-at-rs-250-crore/article67067128.ece visited 2 January 2024
[42] Briefing I, 'India's Digital Personal Data Protection (DPDP) Act, 2023' (*India Briefing News*, 20 December 2023) (https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/ visited 19 January 2024.

The Act's proposal to remove provisions 43A and 87(2) (ob) of the Information Technology Act, 2000 emphasizes this subtle manipulation and suppressing the rights of data principal even further. Section 43A of the IT Act, 2000 is to be repealed by section 44(2)(a) of the DPDP Act, which states that in the event that a body corporate fails to implement and maintain reasonable security practices and procedures when processing, handling, or dealing with any sensitive personal data or information in a computer resource that the said body corporate owns, controls, or operates, an affected person (Data Principal) may demand damages in the form of compensation from the body corporate under Section 43(A) of the IT Act, 2000.[43]

Thus, the government eliminates three issues with one law by preventing a data principal from pursuing compensation under the DPDP Act and by secretly eliminating the two enabling clauses from the Information Technology Act, 2000. The IT Act's provisions have been quashed, which narrows the channels through which impacted parties can seek compensation for data breaches and highlights their precarious position. On a comparison with international standards this stands in stark contrast to the General Data Protection Regulation (GDPR) of the European Union, which firmly guarantees the right to compensation for breaches of personal data. [44]

6. Exclusions of liability and limiting obligation: The Union government is given complete discretion to exclude government agencies and data fiduciaries, including start-ups, from a number of regulations under Section 17. The broad powers granted to government agencies, purportedly based on the preservation of public order, friendly relations with foreign states, security of the State, Indian sovereignty and integrity, or the avoidance of incitement to any cognizable offence related to any of these, raise concerns about the unchecked use of executive power and may cause unwarranted invasions of private rights.[45] The primary goal of the law may be undermined by disproportionate exclusions for government organizations, which might unintentionally make it easier to circumvent data protection requirements.

7. CONCLUSION

The distributive features of privacy laws are frequently downplayed in policy and scholarly discussions in general but now it's more important than ever to categorize them. Privacy implies certain security qualities and security resolves some privacy characteristics, the two constructs are different and have to be handled independently. The interactions between privacy and security in this technologically and increasingly dependent on artificial intelligence driven world show how the necessary trade-offs need taking into account a wide range of circumstances and how the contemporary situational technological environment might alter the relative correlations between the privacy and security features and in the absence of some regulatory mechanism, it might be fatal to individual privacy and user data. [46] Therefore, lack of a legal mechanism controlling a robotics driven technology is not only critical to Right of Privacy guaranteed by the Supreme court but almost always results in privacy concerns around personal data

[43] John Brittas and Aneesh Babu, "What Lies Beneath the PR Blitz on the New Data Protection Act?" (*The Wire*, December 22, 2024) (https://thewire.in/government/what-lies-beneath-the-pr-blitz-on-the-new-data-protection-act visited January 2, 2024.
[44] 'Digital Personal Data Protection Act, 2023 – Key Highlights', 'Digital Personal Data Protection Act, 2023 – Key Highlights' (19 February 2023) visited 19 February 2024
[45] Desai N, 'Demystifying Ai Governance: A Guide For Boardroom Decision-Makers' (Nishith Desai Associates 2024) Visited 18 February 2024
[46]Karthick Theodore v. Madras High Court, 2021 SCC OnLine Mad 2755.

being violated and thus being unsupported by almost all data driven entities. Data privacy, data security, human privacy and individual well being are part of basic freedom, they all only complement one other when there is no anonymity, secrecy and adequate protection of basic fundamental human rights.