RESEARCH COMMUNICATIONS
(An International Open Access, Peer Reviewed, Multidisciplinary Online Journal)
https://research-communications.cmpcollege.ac.in
ISSN: 2584-1270
Volume: 2, Issue: 1, January-June 2024, pp.201-210

Data Protection in India: Digital Personal Data Protection Bill 2022

Renu Singh

Assistant Professor
CMP Degree College, University of Allahabad,
Prayagraj, Uttar Pradesh, India
E-mail: renusingh7732@gmail.Com

Abstract

It has become crucial for businesses to gather more data about their customers without any checks since the development of massive data storage and processing technologies like machine learning and artificial intelligence, which can extract valuable insights for strategic decision-making for businesses. The typical citizen's data use has significantly increased as a result of the spread of internet services to India's most rural towns and villages and the rise in the affordability of smartphones. This paper is an attempt to analyze the data privacy laws in India, with special regards to the Digital Personal Data Protection Bill, 2022. In regards to the Bill many strict compliance standards that should have been looked favorably before have been loosened by the new law. The new regulation is seen as more accommodating and handles "personal data" in a more transparent manner than its predecessor while enforcing strict penalties for infractions.

Keywords: *Data Fiduciary, Data Principal, Consent, Data Privacy, Data Processing and Minimization*

Introduction

Data and the Rising Need of Data Prtoection

"Digital freedom stops where that of the users begins... Nowadays, digital evolution must no longer be offered to a customer in a trade-off between privacy and security. Privacy is not for sale, it's a valuable asset to protect."

– Stephane Nappo
Digital Security Services Activist

The data is information that has been converted into an efficient format for processing or transportation. Data is information that has been transformed into binary digital form for use with modern computers and transmission media. Data now includes records of web activity, logs, and text, audio, and video content.

In a nutshell, data is the fundamental component of both digital and analogue existence in the modern world. Data protection is becoming more and more crucial as the volume of data being generated and stored has grown at an unparalleled rate. Furthermore, since data is becoming more and more essential to company operations, even a brief outage or a tiny quantity of data loss can have a significant impact on an organization.

Internet usage has increased dramatically in the twenty-first century.With nearly 5.07 billion users around the world at present, 692 million users in India[1] alone, this new age phenomenon has given rise to the famous axiom of our times, “data is the new oil”. A number of sovereign organisations have attempted to enact laws pertaining to data protection and safeguarding in an effort to meticulously cultivate, process, and govern the "new gold." The General Data Protection Regulation1 of the European Union is frequently praised as the benchmark for data protection regulations.Several other entities such as Australia, China and the United States of America have attempted to successfully legislate on the usage of data along with the European Union[2].

The endeavor to address digital personal data protection in India has been pursued through the Digital Personal Data Protection Bill, 2022, marking the nation's fourth endeavor at formulating comprehensive legislation in this domain. This scholarly analysis aims to dissect the realms of data protection laws within the unique Indian framework, delving into the nuances of the recently introduced Digital Personal Data Protection Bill, 2022, while critically assessing its limitations. Moreover, this paper seeks to proffer recommendations aimed at surmounting the identified shortcomings inherent in the bill.

Data Protection Laws in India

Right to Privacy

Through the Judicial Lens

Throughout history, various dimensions of privacy have evolved, encompassing the sanctity of one's physical space, bodily autonomy, and personal preferences. In the contemporary digital era, the preservation of these rights assumes heightened significance. Debates have arisen regarding the influence of social media platforms on the landscape of privacy rights within the

[1] Simon Kemp, Digital 2023: India- Data Reportal-Global Data Insights, 13th February, 2023, retrieved https://datareportal.com/reports/digital-2023-global-overview-report.

[2] Available at https://www.scconline.com/blog/post/2023/01/21/the-digital-personal-data-protection-bill-2022/

current digital milieu.

The Supreme Court acknowledged a person's right to protect his privacy in a variety of situations in *R. Rajgopal v State of Tamil Nadu*[3]. The Right to Privacy was acknowledged in *Peoples' Union for Civil Liberties v Union of India*[4], in view of Article 17 of the International Covenant for Civil and Political Rights[5] and Article 12 of the Universal Declaration of Human Rights[6]. The SC acknowledged the Right to Privacy as a crucial component of Article 21 in *Ram Jethmalani v Union of India*[7]. According to *Maneka Gandhi v Union of India*[8], a basic right to privacy can be restricted through a legal process that is just, fair, and reasonable. This right is included in the scope of Article 21's right to life and personal liberty.

The Supreme Court ruled in *State of Maharashtra v Bharat Shanti Lal Shah*[9], that the Right to Privacy can be restricted in accordance with the process duly set by Law. In *Govind v. State of Madhya Pradesh*[10], upon analysis, it was ascertained that the fundamental rights explicitly enshrined for citizens encompass diverse domains, among which the right to privacy stands as an independent fundamental right, albeit subject to constraints rooted in paramount public interests.

Through the examination of pertinent case law, it becomes apparent that the Indian judiciary has progressively broadened the scope of privacy to encompass a wide array of concerns. It is imperative to conceptualize privacy in expansive terms, encapsulating bodily sovereignty and autonomy in decision-making across spheres traditionally regarded as personal.

Statutory Provisions on Data Privacy

The sharing or receiving of personal information in spoken, writing, or electronic form is not protected by a stand-alone legislation in India, though there are safeguards that are spread over a variety of Laws, Regulations, and Rules. Information Technology (Amendment Act of 2008)[11] and Information Technology (Sensitive Personal Data or Information) Rules of 2011[12] include the very basic clauses.

[3]1994 SCC (6) 632.
[4]AIR 1997 SC 568.
[5]1.No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation, 2. Everyone has the right to the protection of the law against such interference or attacks.
[6]*supra* Note 6.
[7](2011) 8 SCC 1.
[8]AIR 1978 SC 597.
[9](2008) 13 SCC 5.
[10]1975 SCR (3) 946.
[11]came into force 27th October 2009.
[12] came into force 28th March 2012.

The Amending Act of 2008 inserted Sec 43A in IT Act, as per which, if: "a corporate body possesses or deals with any sensitive personal Data or information, and is negligent in maintaining reasonable security to protect such Data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected."

Section 72A stipulates the consequences for divulging information in violation of a lawful contract, wherein an individual may face imprisonment for a duration not exceeding three years, or a fine not surpassing five lakh rupees, or both, if found guilty of breaching a lawful contract through information disclosure. The penalties for such actions are delineated in Section 72.It says that: "any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such electronic record, book, register, correspondence, information, document or other material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000 or with both."

Anyone who commits an offense or violation outside of India shall be held to the same standards as anyone who commits an offense or violation in India. This is stated in Section 75 of the Act.

Digital Personal Data Protection Bill- Background

In November, the Digital Personal Data Protection Bill, 2022 was unveiled by the Indian Ministry of Electronics and Information Technology (MeitY). Presented by the Union Minister for Communications, Electronics, and Information Technology, Ashwini Vaishnav, the bill underwent a period of public consultation until December 17, with the deadline subsequently extended to January 2, 2023.

This is our fourth attempt at presenting a data protection bill, and it was proposed after roughly four to five years of delays and revisions. In 2017, the country's Supreme Court ruled that privacy was a basic right protected by the Indian Constitution[13]. In light of this ruling, the top court requested that the government establish a set of data protection regulations.

The government then established an expert group under the direction of Sri BN Sri Krishna, a retired judge of the Supreme Court. A year later, the committee presented a draft of the Data Protection Bill along with its report, and the Ministry of Electronics and IT announced that it would draw inspiration from the former Justice Sri Krishna Committee's ideas to develop the legislation.

[13] *K.S. Puttaswamy v. UOI,* (2017) 10 SCC 1.

Additionally, it has been noted that the Digital Personal Data Protection (PDP) Bill encountered significant resistance from various stakeholders, including prominent technology firms such as Facebook and Google. This opposition primarily stemmed from the bill's inclusion of data localization provisions, which would restrict these companies from exporting unspecified personal user data and mandate the retention of specific sensitive information within the nation's borders.

In addition, the Joint Parliamentary Committee suggested 81 amendments (in a 99-section bill) and 12 recommendations after 78 sittings, more than 184 hours, and numerous extensions[14]. According to reports, privacy and civil society advocates criticized the bill's delays because one of the nations with the highest per-capita data consumers and producers lacked a fundamental legal framework to safeguard internet users' privacy.

Digital Personal Data Protection Bill- Key Principals

Firstly, usage of personal data by organizations must be done in a manner that is lawful, fair to the individuals concerned and transparent to individuals.

Secondly, personal data must only be used for the purposes for which it was collected.

The third principle talks of data minimization[15].

The fourth principle puts an emphasis on data accuracy when it comes to collection.

The fifth principle talks of how personal data that is collected cannot be “stored perpetually by default” and storage should be limited to a fixed duration.

The sixth principle says that there should be reasonable safeguards to ensure there is “no unauthorized collection or processing of personal data.”

Seventh principle states that “the person who decides the purpose and means of the processing of personal data should be accountable for such processing.”

The Bill would be applicable to the handling of digital personal data processed in India[16], whether the data is obtained online or offline and then converted to digital form. If the processing is being done to sell products or services or create profiles of people in India, it will also apply to processing done outside of India.

Only legitimate uses of personal data may be carried out with the agreement of the data subject. In some circumstances, consent may be assumed. Data fiduciaries will be required to keep data

[14] Graham Greenleaf, India – Confusion Raj with Outsourcing in Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2017) at p. 415.
[15] retrieved https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.
[16] Section 5 of the Bill.

accurate, safe, and deleted when its purpose has been served.

The Law provides individuals with a number of rights, including the ability to request information, seek rectification and erasure, and file a grievance.

Scope of the Bill

Every ‘digital personal data’ processed within India is subject to the Bill. For the purpose of understanding, the term 'data' is used in the Bill to mean the “representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means”[17], while the term 'personal data' is defined as 'any data about an individual who is identifiable by or in relation to such data'. According to the Bill, the phrase "digital personal data" refers to both data gathered offline and afterwards converted to digital form as well as data acquired online by a ‘Data Principal’ (viz. the individual to whom the personal data processed is in relation to). Particularly, if such a private person is a ‘child’ (i.e., less than 18).

It is noteworthy to emphasize that the Digital Personal Data Protection (PDP) Bill possesses a territorial jurisdiction that extends beyond the confines of India, encompassing digital personal data handled beyond its borders under specific circumstances. These circumstances include scenarios where data processing is conducted for the purpose of selling products or services to individuals within India, as well as instances where personal data is processed explicitly for the practice of "profiling" or analyzing factors related to an individual's behavior, characteristics, or interests.

Notably, the bill excludes personal data handled in "offline" settings from its purview. Moreover, it explicitly exempts certain categories of data, such as data processed by individuals for personal or domestic purposes, personal data contained within records existing for at least a century, and data subject to "non-automated processing," also referred to as manual processing.

Key Definitions and Analysis

Data Fiduciary and Consent

A "Data Fiduciary" is a legal term used to describe an organization that is not currently named or covered by Indian law. Under the DPDP Bill, the term "Data Fiduciary" has been introduced to describe a person who, individually or jointly with others, "determines the purpose and means of processing" personal data in accordance with Data Principles. This definition includes both natural persons (such as any individual) and artificial or juristic persons (such as a company, firm, or other organization).

[17] Section 2(4) of the Bill.

Every statement or action that unequivocally demonstrates that a Data Principal has consented to the processing of his or her personal data must qualify as consent. In order to get this consent, Data Fiduciaries are required to send relevant Data Principals (including even those whose consent was received previous to the introduction of the DPDP Bill) a notification that, among other things, specifies the data that is intended to be gathered[18]. Moreover, in response to such notice, a specific request for the relevant person's consent must be made (in the prescribed format). For this reason, Data Fiduciaries must first name a "Data Protection Officer" (whose information must be provided with the Data Principal.

Moreover, Data Fiduciaries are required to show evidence of the notice's delivery or the Data Principal's approval (in the event of a judicial challenge by the relevant Data Principal)

However, the Digital Personal Data Protection (DPDP) Bill introduces the concept of "deemed consent" under specific and limited circumstances, wherein the consent of a Data Principal is considered inherently necessary. These circumstances encompass instances where a Data Principal is evidently obligated to provide personal information to a Data Fiduciary for lawful purposes, such as accessing beneficial services or obtaining licenses, certificates, or permits. Additionally, deemed consent applies in situations necessitated by compliance with judicial orders, employment-related requirements, matters concerning the public interest, and other purposes deemed "fair and reasonable."

Also, whether the consent requirement should apply where government agencies providing commercial services is disputed.

As outlined in the Bill, the consideration of consent is paramount when the State and its instrumentalities engage in data processing activities to provide benefits and services. Consent requirements afford individuals control over the extent of data collection and processing. This provision encompasses government entities and public sector utilities offering a variety of services to the populace, spanning sectors such as power, banking, healthcare, and telecommunications. Consequently, government health agencies, entities like SBI, BSNL, and state distribution companies are not mandated to obtain individual authorization prior to processing their data.

However, the appropriateness of this approach is subject to scrutiny and debate.The Sri Krishna Committee (2018) had observed that there is an imbalance of power between the individual and the State if the State is the only provider of a service or benefit.[19]

[18] Section 6(1) and 6(2) of the Bill.

[19]A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Sri Krishna, July 2018.

Right to Correction and Erasure Vs The Right Be Forgotten

The right to data portability and the right to be forgotten are not covered by the Bill. Both the 2019 Bill that was tabled in Parliament and the 2018 Draft Bill attempted to provide these rights.[20] After looking at the 2019 Bill, the Joint Parliamentary Committee suggested keeping these rights. These rights are likewise acknowledged by the General Data Protection Regulation (GDPR) of the European Union. A robust set of data primary rights, according to the Sri Krishna Committee's (2018) findings, is a crucial element of a data protection legislation. To provide people control over their data, these rights are founded on the concepts of autonomy, transparency, and accountability[21].

Right to Data Portability: The right to data portability allows data principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format. It gives the data principal greater control over their data and can facilitate the migration of data from one data fiduciary to another. One possible concern has been that access to such information may reveal trade secrets of the data fiduciary.

Right to be Forgotten: The right to be forgotten is a concept that seeks to impose memory constraints on an otherwise infinite digital realm, according to the Sri Krishna Committee (2018). 4 The Committee did emphasize that this right could need to be weighed against other rights and interests, though. The exercise of this right may conflict with another person's freedom of expression and informational rights. 1 Its application may depend on elements including the sensitive nature of the restricted personal data, the significance of the data to the public, and the purpose of the data.

Data Protection Board of India

The DPDP Bill provides for formation of a regulatory body termed as the 'Data Protection Board of India'. The Bill mentions that the primary function of the Board is to determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act. The Law further stipulates that subsequent regulations would be made regarding the composition, strength, incidental qualifications, selection method, periods of appointment, and dismissal of the chairman and other members[22] (i.e. potentially under the Rules which will be published once the Bill is passed in the parliament). The Bill further stipulates that the Central Government would designate the Chief Executive of the Board, and that the Chief Executive's terms and conditions of employment would be as the Government may choose.

[20] Clause 26, The Personal Data Protection Bill, 2018, as released by Ministry of Electronics and Information Technology.
[21] Article 20, General Data Protection Regulation, European Union.
[22]Ashneet Hanspal, Aditi Mendiratta, Gaurav Bhalla, India: Analysis Of The Digital Personal Data Protection Bill, 2022.

The issue is whether these specifics have to be included in the main law to guarantee the Board's independence.

The Board's primary responsibilities include: I identifying violations of the Bill's requirements; (ii) levying fines; and (iii) requiring data fiduciaries to take the appropriate action in the event of a data breach. Governmental organizations may frequently be the target of such inquiries due to the volume of personal data they handle. This casts a doubt whether the Board will be able to act independently in such a situation.

Conclusion

The Digital Personal Data Protection (DPDP) Bill allows the Central Government the authority to exempt certain Data Fiduciaries or categories of Data Fiduciaries from specific provisions outlined in sections 6(2) and (6), 9, 10, and 11 of the Bill, contingent upon the volume and nature of personal data handled. Under Provision 12 of the Bill, when a Data Principal requests specific data, informed Data Fiduciaries are exempted from the obligation to furnish such information. However, there is a concern that this provision may inadvertently undermine the powers granted to Data Principals, particularly when dealing with large datasets.

The ambiguity surrounding the concept of privacy complicates the delineation of behaviors that constitute a breach of this fundamental right. Organizations, especially those with headquarters both in India and abroad, accumulate vast amounts of data. To obtain users' consent for data collection and storage, organizations often incorporate the notion of informed consent into their terms of service agreements. However, there remains a veil of uncertainty regarding the scrutiny and utilization of this amassed data.

Therefore, it is imperative for the drafters of the Bill to reassess these aspects to ensure that there is no room for arbitrary actions. Measures should be taken to strengthen the safeguards protecting Data Principals' rights, even in the face of extensive data handling practices. Additionally, greater clarity and specificity should be introduced to the provisions pertaining to consent and data processing, thereby fostering transparency and accountability within the digital ecosystem.

Acknowledgement

I would like to express my deepest appreciation to PRS Legislative Research journal. I also could not have undertaken this journey without my peers at CMP Degree College, Prayagraj, who generously provided with all the knowledge. I am also grateful to them for their editing help and moral support. Thanks should also go to the study participants from the university, who impacted and inspired me. Lastly, I would be remiss in not mentioning my parents. Their belief in me has kept my spirits and motivation high during this process.

References

A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.

Ashneet Hanspal, Aditi Mendiratta, Gaurav Bhalla, India: Analysis of the Digital Personal Data Protection Bill, 2022.

Graham Greenleaf, India – Confusion Raj with Outsourcing in Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2017).

Harrington, D, U.S. Privacy Laws: The complete guide, Varonis, (2022, September), Retrieved from https://www.varonis.com/blog/us-privacy-laws.

Simon Kemp, Digital 2023: India- Data Reportal-Global Data Insights, 13th February, 2023, retrieved https://datareportal.com/reports/digital-2023-global-overview-report.