Page 673 - 682 **DOI:** *https://doij.org/10.10000/IJLSI.111344*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 4 | Issue 1

2022

The Personal Data Protection Bill, 2019: An Analysis

ANISHA SHARMA[1] AND TRISHAN DOLLNY[2]

ABSTRACT

Data is all around us. The creation and storage of data are growing at unprecedented rates. They are changing the face of the world. There is no denying that data generation and its ease of retrieval has contributed to the development of a fast-paced, tech-savvy society. However, in the process of providing society with the benefits of technological advancements, valuable personal information about individuals or their personal data is not always protected from unauthorised access and is often misused, resulting in a violation of peoples' right to privacy. Therefore, personal data needs to be protected, along with maintaining the privacy of those who manage the data, that is, the data principals.

There are no specific laws for data protection in India. Therefore, an expert committee, headed by B N Srikrishna, a retired judge of the Supreme Court, was set up to draft a Personal Data Protection Bill. This draft bill was submitted to the Ministry of Electronics and Information Technology, post which the then Minister of Law and Justice, Electronics and Information Technology and Communications, Mr Ravi Shankar Prasad, introduced a revised Personal Data Protection Bill in the Lok Sabha in 2019. This paper deals with how the revised bill has jeopardised the fundamental right to privacy which was recognised in the case of K S. Puttaswamy v. Union of India in 2017.

The paper also makes a comparative analysis of the Personal Data Protection Bill, 2019 with the European Union's General Data Protection Regime Model Regulation (2018), on which both the draft and the proposed versions are based. After that, the paper gives some recommendations for the revised bill to ensure its consonance with the intent to protect data, respecting the right to privacy, as well as for its effective and efficient implementation.

I. UNDERSTANDING WHAT THE TERM "PERSONAL DATA" ENCOMPASSES

According to the EU General Data Protection Regulation, better known as the GDPR, **personal** data is any piece of **information** that is directly related to a person and can be used to identify that person as it is unique to him/her. Art. 4(1) of the GDPR defines 'personal data' as "***any***

[1] Author is a student at National Law University, Delhi, India.
[2] Author is a student at National Law University, Delhi, India.

 [ISSN 2581-9453]

information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[3] Examples of information that come under the category of personal data are telephone, credit card or personal numbers of a person, or vehicle number plates registered under a person's name, an individual's bank account data, customer number, address or even appearance.[4]

The **Personal Data Protection Bill**, 2019 (hereinafter referred to as the PDPB) recognises three different categories of data, which are (1) Personal Data, (2) Sensitive Personal Data, and (3) Critical Personal Data. Section 3(28) of the PDPB states that **"*personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.*"**[5] The definition of 'personal data' in the PDPB is similar to that in the GDPR as it encompasses the identity and attributes of a natural person or information that can be utilised to directly or indirectly identify a natural person. Reflecting on the term *indirectly identifiable*, a thought might arise regarding the scope of personal data because to *directly* identify a natural person from data would in itself be a confirmation that the data was personal. However, in the case of *indirect* identification, a *combination* of different pieces of information would most probably be used to identify a person. If so, the question arises whether this data was truly personal to begin with and if such data can be considered personal, then what comes under the category of non-personal data? Such issues could pose a challenge for data principals, as well as serve as opportunities for enforcing agencies to access personal information under the guise of non-personal data.

Sensitive Personal Data includes "***financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator."***[6] This essentially means that the government can further broaden the scope of sensitive personal data by adding more categories. However, when it comes to Critical Personal Data, the PDPB is even less specific, as it vests the Central Government with the power to define and determine the nature of critical personal data. Clear and specific definitions would be preferred to prevent varied interpretations and possible misuse.

[3] EU General Data Protection Regulation, art. 4(1).
[4] Intersoft Consulting, https://gdpr-info.eu/issues/personal%20data/ (last visited Aug 10, 2020).
[5] The Personal Data Protection Bill, 2019, § 3(28).
[6] PRS Legislative Research, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 (last visited Aug 10, 2020).

II. WHAT ARE DATA PROTECTION AND DATA PRIVACY?

Data protection and data privacy are often confused with being the same. However, data protection is the mechanism of safeguarding information of users/clients from unauthorised parties accessing it and is a technical matter. On the other hand, privacy is defining who or which entities have the authority to access particular pieces of information and is a legal and/policy-decision matter, not a technical one. A very important distinction between data privacy and data protection is made on the basis of who controls both these aspects. It is imperative to note that the data principals are in control of data privacy as they decide which piece of information can be shared and with whom. However, it is the data fiduciaries who are in charge of data protection to ensure that they maintain the level of privacy a data principal consents to/establishes. Data fiduciaries make sure that the information does not land up in the hands of unauthorised entities. Another distinction between data protection and data privacy is that data protection prevents hackers from accessing your information, whereas data privacy prevents your data from being shared and/or sold. Both data privacy and data protection go hand in hand, as the former decides which information can be used by whom and for what purpose, whilst the latter maintains the level of privacy set by the data principal. A global survey[7] conducted in 2019 by Comparitech, a UK-based research firm, ranked India as the third-worst in data privacy, only after Russia and China.

III. RIGHT TO PRIVACY AND THE PERSONAL DATA PROTECTION BILL, 2019

The right to privacy is recognised under Article 12 of the Universal Declaration of Human Rights[8], Article 17 of the International Covenant on Civil and Political Rights[9] and Article 8 of the European Convention of Human Rights[10]. It was recognised as a fundamental right, enshrined under Article 21 of the Constitution of India[11], in the case of *KS. Puttaswamy and Ors. vs. Union of India and Ors.*[12] (the *Puttaswamy* case). The Supreme Court stated that the right to privacy is inseparable from and intrinsic to the human element and core of human dignity.[13] The right to privacy has both positive and negative elements. The negative element prevents the State from intruding on a citizen's life and personal liberty, while the positive element requires the State to take all reasonable measures to protect the individual's privacy.[14] As a result, the constitutional protection of privacy may give rise to two interrelated protections:

(i) against the world at large, to be respected by all, including the State: the right to choose what personal

[7] Paul Bischoff, 'Surveillance States: Which countries best protect privacy of their citizens'(Comparitech Blog, 15 October 2019) 2020.
[8] Universal Declaration of Human Rights, art. 12.
[9] International Covenant on Civil and Political Rights, art. 17.
[10] Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8.
[11] Indian Constitution, art. 21.
[12] K.S. Puttaswamy and Ors. vs. Union of India and Ors., (2017) 10 SCC 1.
[13] *Id*. at ¶ 459.
[14] *Id*, at ¶ 403.

information is to be released into the public space; and

(ii) against the State, as a necessary corollary of democratic values, limited government, and limits on State power.[15]

However, the right to privacy is not an absolute right. It is subject to numerous restrictions such as procedures established by law that must be just, fair, and reasonable; if it is in the interest of India's sovereignty and integrity; not available to persons who voluntarily thrust herself/himself into controversy; if there is a significant countervailing interest that is superior; and if it is against the interests of private citizens.[16]

Currently, the average person, or in this case the consenting authority/data principal, isn't fully aware of the scope of his/her right to privacy. There is a major issue of privacy being breached, as data principals are unaware about what entails the terms and conditions that they agree to at the time they provide their personal information, or what the information is being used for, by whom, and for how long.

The PDPB, presented in the Lok Sabha, incorporated modifications from the original draft, two of which are discussed herein. *Firstly*, the list of data fiduciaries was extended to include social media intermediaries who enable online interaction and those that have a certain number of users. *Secondly*, the scope of exemptions for the State was extended, which will enable the State agencies to collect anonymised personal as well as non-personal data from data fiduciaries, thereby giving the State unrestricted access. The nature of such exemptions can be interpreted as a violation of the fundamental right to privacy and may be argued to be unconstitutional. Therefore, it is imperative to analyse the provisions of the PDPB in light of the privacy principles laid down in the *Puttaswamy case.*

Specifically, sections of the revised PDPB that raise doubts on its constitutionality are:

Section 35 of PDPB

Section 35 of the PDPB, which empowers the Central Government to exempt "any" agency of the government from the application of "all or any" provisions of the Act, with regards to processing personal data, **"(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognisable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order".[17]** Section 35 does not enlist or establish any conditions that must be fulfilled before allowing a government agency to avail this exemption under the provisions of the Act.

The above issue posed by Section 35 did not exist in the draft bill of 2018, as **section 42 of the draft bill[18]** exempted government agencies from the

[15] *Id*, at ¶ 304-307.
[16] Neelam Rai, Right to Privacy and Data Protection in the Digital Age - Preservation, Control and Implementation of Laws in India, 11 INDIAN J.L. & Just. 115 (2020).
[17] The Personal Data Protection Bill, 2019, § 35.
[18] The Personal Data Protection Bill, 2018, § 42.

provisions of the draft bill, only in the interests of the security of the State and established four conditions, namely:

- it was authorised pursuant to law.
- it was in accordance with the procedure established by such law, made by Parliament.
- it was necessary for achieving such interests.
- it was proportionate in its application.

However, PDPB gives absolute power to the Central Government to exempt its agencies from privacy restrictions if it believes that it is essential or expedient to do so, thereby enabling the Central Government to act solely on the basis of its own rationality. This excessive power is potentially a grave threat to the privacy of India's data principles. In the *Puttaswamy case*, it was held that the fundamental right to privacy encompasses informational privacy and therefore recognises that an individual can set the level of privacy pertaining to information that is personal. Therefore, it is imperative to keep a restriction on access to personal information, as that is the only way to protect our fundamental right to privacy. To ensure the safety of our fundamental right, specific conditions akin to the now-removed section 42 of the draft Bill of 2018 need to be established under which the State would access personal data. These conditions would be over and above the permissible purposes already mentioned, such as sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order. Additionally, it is worthy of mention that in the *Puttaswamy* case, it was held that unauthorised use of such information might lead to infringement of the individuals' rights as the right to privacy is based on the concept of consent.

However, data principals too must recognise that fundamental rights are subject to restrictions that are fair, just and reasonable. Any infringement of the right to privacy must satisfy the *State-interest Test,* which was devised by Justice Chandrachud, to ensure that the government's powers are kept in check. *The State-interest Test* is a three-fold test to justify the violation of any kind of privacy (not just informational privacy), and the three conditions it lays out are **(1) existence of law, (2) legitimate state aim and (3) proportionality.** The condition of proportionality ensures that any action by the State/breach of privacy by the State is not disproportionate to the purpose of the law in that particular circumstance.[19] Proportionality is a condition that plays an imperative role in protecting data principally from arbitrary actions of the State.

As explained above, this lack of constraint over the ambit of Section 35 and simultaneous removal of Section 42 from the PDPB, together, raise the issue of constitutionality surrounding Section 35. If construed without regard for principles under the *State-interest Test*, Section 35 could effectively grant unrestricted power to the State in assessing whether the fundamental right to privacy can be infringed. This sweeping power could be problematic because it raises

[19] K. S. Puttaswamy v. Union of India, AIR 2017 SC 4161, ¶ 180.

 [ISSN 2581-9453]

genuine concerns with regards to citizens being spied on, as it allows the State to access any information, which under normal circumstances it would have no authority to access. The information thus accessed can be extremely dangerous because, as seen in *Radhakrishna v. State of Uttar Pradesh*[20], such data becomes admissible evidence overlooking the breach of privacy.

Section 91 of PDPB

Section 91 of the Personal Data Protection Bill 2019 authorises the government to frame any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, provided that such policy does not govern personal data. Additionally, it allows the Central Government, in consultation with DPAI (Data Protection Authority in India), to direct data fiduciaries to provide it with any 'anonymised' personal data or non-personal data.[21]

Section 2(b) states that the provisions of the Act do not apply to anonymised data "other than anonymised data referred to in section 91".[22] Section 91 goes further, allowing the State to obtain data from data fiduciaries without the data principal's consent or restrictions. This enables the State to direct data fiduciaries such as *WhatsApp, Amazon, Google, Twitter, Facebook, and Snapchat* to divulge user data. Lack of transparency and accountability will always keep data principals in the dark, and they may never know the purpose for which their personal information may be used. This violates the principle of consent laid down in the *Puttaswamy case;* since Section 91 relinquishes the need for consent, data principals have no way of knowing how or for what purpose their personal data may be utilised. This grants unrestricted powers to the State, which is beyond being fair and reasonable.

As discussed earlier, Section 3(28) of the Bill defines 'personal data' as information that directly or indirectly identifies a natural person or relates to any characteristic, trait, or attribute of that person.[23] Since 'non-personal data' has not expressly been defined in PDPB, it is possible that the wide nature of these definitions might be interpreted to access personal data, purporting it to be non-personal data. Even access to non-personal data comes with a possible risk that, with the help of technology, data can be re-identified. What these options effectively imply is that the State can access personal information, generating considerable concerns about the confidentiality of data supplied to data fiduciaries by the principals. Another reason why the specificity of definitions is important can be illustrated with reference to online target advertising, where certain organisations track online activities conducted by people to control the advertisements that they get to see. On the face of it, this might be viewed as a beneficial tool for the data principal, as it allows the data principal to see relevant advertisements/data gathered from one's online activities and at the same time may be considered to be relatively

[20] Radhakrishna v. State of Uttar Pradesh, AIR 1963 SC 822.
[21] The Personal Data Protection Bill, 2019, § 91.
[22] The Personal Data Protection Bill, 2019, § 2(b).
[23] *Supra* note, 3.

harmless insofar as enabling the identification of an individual is concerned. However, there is a risk that multiple pieces of data may be put together like a puzzle to identify the data principle.

Section 41 of PDPB

Section 41 of PDPB establishes the Data Protection Authority in India ('DPAI') to protect the interests of data principals, prevent any misuse of personal data, ensure compliance and promote awareness about data protection.[24] It is to be independent and autonomous. However, the appointments to the DPAI are to be made by a selection committee comprising the Cabinet Secretary, Law Secretary and Electronics and Information, and Technology Secretary. Salaries and tenure are also to be decided by the Central Government. This may undermine the independence of DPAI and possibly makes the members of DPAI acquiescent to the needs and orders of the government instead of protecting the privacy rights of the people, thereby defeating its purpose.

Therefore, the requirement to consult the DPAI before notifying any data as sensitive personal data under section 33 of the PDPB is indirectly coming under the sole and exclusive power of the Central Government as DPAI is functioning entirely under the control of the government.

This is extremely bothersome as a number of Central Government agencies are themselves data fiduciaries, under PDPB and may soon become the largest data processor in the country. Therefore, they can take advantage of their unfettered and absolute power to satisfactorily fulfil their interest as data fiduciaries. The Central Government can interpret the definitions of these terms so as to benefit their agencies.

The PDPB has effectively taken power from the Parliament and thrust it upon the Central government to decide who will form part of the exemptions from following the Act, which implies that there will be no debate, discussion, contrarian opinions or even opposition about the exercise of discretion.

Section 33 of PDPB

Section 33 of PDPB provides that "sensitive personal data" can be transferred outside India. However, such data must necessarily be continued to be stored in data centres located within India. Section 33 also prohibits "critical personal data" from being processed outside of India. However, "critical personal data" is defined as the data which is to be notified as critical personal data by the Central Government.[25] Before notifying certain forms of personal data as sensitive personal data, the Central Government must consult with DPAI. However, the independence of DPAI itself is suspect, as discussed in the foregoing paragraphs above. Effectively, what this means is that the government has the sole power to notify “critical personal data”. Such unbridled powers granted to the government in PDPB cannot be said as just, fair and reasonable.

[24] The Personal Data Protection Bill, 2019, § 41.

[25] The Personal Data Protection Bill, 2019, § 33.

IV. COMPARATIVE STUDY: GDPR AND PDPB

Article 45(2)(b) of the GDPR, while assessing the adequacy of data protection, envisages "independent" supervisory authorities to ensure and enforce data protection rules.[26] Article 52 of the GDRP clarifies that "each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this regulation". Additionally, Article 52 confers the power upon the supervisory authority to choose its own staff members so as to ensure that the financial control over the supervisory authority does not affect its independence.[27]

Section 41 of PDPB provides for the establishment of an independent and autonomous authority to ensure and enforce data protection rules. However, the independence of the authority is delusional in India because the powers for appointment and removal of members of the DPAI are vested solely in the central government, according to sections 43 and 44 of PDPB, respectively.

Article 33 of the GDPR[28] requires notifying of a personal data breach to the supervisory authority. The data fiduciary has to inform the supervisory authority of this data breach without undue delay and within 72 hours of becoming aware of it. **Article 34** requires the controller to communicate the data breach to the data principal in case the breach is likely to result in significant risk to the rights and freedoms of the person.[29] GDPR imposes a duty on the data fiduciary to notify the supervising authority and, in select cases, the individual in cases of a data breach. All efforts are taken to mitigate the effects of such a breach also have to be documented.

Section 25 of PDPB imposes a duty on the data fiduciary to inform the DPAI in case of breach of any personal data that may cause harm to the data principal, and it is up to the DPAI to inform the data principal about the breach at its own discretion.[30] The particulars, including remedial measures being taken by the data fiduciary, have to be included in the notification to the DPAI.

Usually, in the case of a data breach, the company or organisation which has had its security compromised will be the first one to know about it, provided that its regulations are in order and the compliance framework is up to date. The organisation, to protect its own interest, will be the quickest to know what damage has occurred and what consequences the breach can have on the data principals via its own assessment. Therefore, the data fiduciary might be in the best position to mitigate the consequences of the breach by informing its data principals at the earliest of the events that have unfolded and what steps will be taken by the fiduciary to deal with it, as well as the preferred methods the data principal should adopt in order

[26] EU General Data Protection Regulation, art. 45(2)(b).
[27] EU General Data Protection Regulation, art. 52.
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).
[29] EU General Data Protection Regulation, art. 34
[30] The Personal Data Protection Bill, 2019, § 25.

to minimise the damage at his end. It is likely that the fiduciary, itself, may be best placed to advise its clients about the protection of data and aim to have water-tight security so that no loose ends are left on its behalf it's Its reputation is also at stake.

Whilst the importance of reporting to DPAI cannot be undermined, it is worth mentioning that DPAI's role should not be reduced to bureaucratic red tape, which would slow down the rate at which the data principal and the data fiduciary can take remedial action. The role of DPAI should serve as a deterrent to conceal data breaches and instil the concept of compliance with laws and regulations. Therefore, to make the procedure more efficient, effective and transparent, both the DPAI and the data principal should be informed by the data fiduciary about the breach of data simultaneously.

V. CERTAIN RECOMMENDATIONS FOR THE PDPB ARE

1. Rules should be made so as to make it compulsory for the data fiduciary to inform and alert the principal in case of any data breach.[31] This line of communication between the data fiduciary and the principal would not only help to protect a data principal's data but also promote transparency between the two.

2. Data fiduciaries, including the government, should send a notice asking for the principal's consent before using its personal data. The procedure and framework must be such that technological laymen would not be tricked into or perplexed by the variety of options available on an online portal and should easily understand what they are consenting to.

3. An independent and autonomous authority should be established – salaries and tenure should be decided by Parliament, not by the Central Government. The selection committee should consist of experts or be formed by a board made up of parliamentarians from both the governing party and opposition parties.

4. PDPB must include conditions such as those akin to the now-removed section 42 of the draft Bill of 2018 in order to keep a check on the Central Government's access.

5. Data fiduciaries, while asking for consent to access a data principal's information, must state the purpose the data is being collected to provide surety that data is only accessed until the purpose is fulfilled. Additionally, a data principal's data must only be shared with a third party after receiving consent from the data principal, and such data must only be shared in an anonymised form to the extent possible. These rules should apply to all data fiduciaries, including the Central Government.

6. The most important factor that guarantees citizens their fundamental right to privacy is being informed about it. It is essential for the government to disclose the intent of PDPB and spread awareness about the rights every data principal in India has. This can be done by creating a website dedicated to

[31]Yash More & Shailendra Shukla, Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy, 6 INDIAN J.L. & PUB. POL'y 42 (2020).

informing a data principal about his/her rights with the help of articles and/or videos.

7. PDPB needs clarity on the term 'any business that is carried out in India' in relation to the exercise of jurisdiction over any data fiduciary or data processor not located within India. Currently, this aspect is vague in nature and lacks specificity.[32] Therefore, to tighten the scope of PDPB and bring in more specificity with respect to its applicability, the above term should be defined clearly or explained.

VI. CONCLUSION

In conclusion, one must understand that the introduction of PDPB is much awaited. Currently, this area of the law is largely governed by the IT Act, which was introduced in the year 2000, and amended only once in the year 2008, ignoring the rapid rate at which technology has advanced in this period, rendering it outdated. Moreover, judging by the rapid rate at which technology is continuing to evolve, it would be imperative for the PDPB, if implemented, to be continuously updated and amended as per the requirements of the data principals of the country. Having said that, it will be a mammoth task to decide what changes to make and when; after all, if the law is changed too often, it will be difficult for people to keep up and follow it. The only way to resolve this issue is to make sure that even if the law has to be revised, its principles and intentions remain unchanged.

Another aspect that must be looked into before implementing PDPB to ensure its true intent is protected is that the powers and exemptions that are provided to the State should be subject to constitutional conditions or restrictions. Not only is this the only way the fundamental right to privacy can truly be upheld, but it is also a mechanism for the citizens of India to retain their trust in the government. In essence, personal data should be processed with transparency over its control and usage, providing necessary privacy to the data principals, whilst enabling ease of access to legitimate and justified users.

*****

[32] The Personal Data Protection Bill, 2019, § 2.