View and Suggestions on the Personal Data Protection Bill, 2019 for the consideration of the Joint Parliamentary Committee of the Parliament (December 2019).

Prepared by the Reading Group on Constitutional Law at Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi.

Names of the members participated:

1. Prabhat Mishra
2. MandiraNarain
3. Anuradha Singh
4. Manpreet Dhillon
5. Deepa Kansra
6. Nupur Chowdhury
7. P. Puneeth

I INTRODUCTION

The Personal Data Protection Bill, 2019 (PDPB)seeks to strike a balance between protection of personal data (privacy of individuals, rights of individuals whose data is processed, establishment of DPA, accountability of fiduciaries etc.) and fostering digital economy (norms for SMIs, creating a framework of technical and organisational measures for data processing).

Prima facie, although the Bill contains certain safeguards for protection of personal data of varied nature, by providing for many blanket exemptions to the State, in particular, it seems to have watered down the efficacy of the safeguards provided to a significant extent. Since the State itself is a data fiduciary, with largest amount of data of citizens/residents under its control, providing blanket exemptions to the State from requirement of compliance with the safeguards would undermine and in some respect defeat the very objectives of the Bill.

In the present scenario where data collection and processing using new technologies are being undertaken by the State in the form of Centralized Monitoring System (CMS) and nation-wide Automated Facial Recognition System (AFRS) etc., the State itself isthe most 'significant data fiduciary' and, therefore, it should not be allowed to seek exemption from compliance with the provisions of the Bill aiming at safeguarding of personal data. It may be noted that the State is under a constitutional obligation to protect the right to privacy of all natural persons as envisaged by the Hon'ble Supreme Court of India in K. S. Puttaswamy v. Union of India (2017).

We provide general comments on the Bill drawing on necessary provisions and statutes for data protection.

II GENERAL THEMES

1. Inconsistency with Srikrishna Committee Recommendations (2018) and law laid down by the Supreme Court in K.S. Puttaswamy (2017).

The PDPB is purported to be based on the foundational principle of the Right to Privacy, a fundamental right as recognized in the *Justice K S Puttaswamy v. Union of India* [(2017) 10 SCC 1]. In Puttaswamy, the Supreme Court listed the four-fold standard of review, which are -"legitimate purpose", "proportionality", "necessity" and "procedural safeguards against abuse". However, the PDPB under Clause35 empowers the Central Government to exempt any government agency from application of the Act. These agencies could be of any nature and not necessarily perform functions of security and public order as permissible under reasonable restrictions. Such provisions conferring wide powers that allow for blanket exemptions to the State are vaguely worded and fail the test of 'legitimate purpose'. Clause 36, which provides for exemptions of certain provisions for processing of personal data also undermines the standard of 'proportionality and standard of necessity'. Similarly, the exemptions given to the State under the PDP are far wider than what was recommended by the Srikrishna Committee in 2018.The Shri Krishna Committee recommendations are more conformity with the law laid down in Puttaswamy whereas the PDPB fails to do so. Therefore, broad and ambiguously worded exemptions granted to the State, further falters on the basic safeguards of protecting civil liberties in the case of the State- Citizen interaction.

2. Incoherent Legislation

PDPB seems to be an inconsistent piece of legislation containing several provisions that do not speak to each other. Some of the provisions in the Bill appear to be irreconcilably inconsistent. For instance:

(i) Clause 9 of the PDPB obligates the data fiduciary "not to retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing." The word used is 'shall' and it suggests the mandatory nature of the provision. Clause 20, on the other hand, confers a right on the data principal to ask the data fiduciary to restrict or prevent disclosure of his personal data where such disclosure has served the purpose for which it was collected or is no longer necessary for the purpose. The same can be enforced only on an order of the adjudicating officer made on an application filed by the data principal.

If the data fiduciary is obligated to delete data after the purpose is served and if it is no longer available with them, what is the need to confer a right on the data principal to seek its non-disclosure when such data is not supposed to be retaining by the data fiduciary.

(ii) It is not clear as to whether provisions contained in clause 17 are applicable to cases covered under clause 19 as well.

(iii) It is not clear whether the compliance with safeguards provided clause 7 is required for exercising powers conferred under clause 12.

3. Misleading nature of the 'Right to be forgotten'

The right to be forgotten is essentially a right to seek erasure of data(Article 17, EUGDPR), The right to be forgotten envisaged under clause 20 of PDPB resembles more of aright to seek non-disclosure with no guarantee of data erasure. Furthermore, under clause 20 (2), there are too many conditions attached to the exercise of this right. The provision is nebulously worded in terms of illustrating the grounds on which the right to be forgotten will not be granted to the data principal. These grounds include the data principal's right in conflict with right to free speech and expression and right to information of any other citizen. Both, the right to privacy and the right to information has been recognised as the fundamental civil liberties but the right to privacy (as is stated in the title and the introduction to the bill) as the PDP Bill, 2019 aims at seemingly gets overridden by someone else's right to information of the personal data of the Data Principal. Additionally, under Clause 20(3)(e)another ground for the review of application has been to assess "if the activities of the Data Fiduciary will be significantly impeded". This prioritises the interests of the Data Fiduciary over the Data Principal's right to privacy and right to be forgotten which is in conflict with the aim of the Bill.

4. Discretionary powers of the Data Fiduciary and Data Protection Authority (DPA)

Clause (7) prescribes the "requirement of notice for collection or processing of personal data". Clause 14 (1), on the other hand, grants excessive powers at the hands of Data fiduciary to process the data for "other reasonable purposes" on vague ground such as, "whether Data Fiduciary can reasonably be expected to obtain the consent of the Data Principal". The grounds for both, 'other reasonable purposes' (see, Clause 14 (2)) and 'any public interests' (see clause 14 (1) (c)), broadens the circumstances where the approval of consent for the processing of the personal data of the Data Principal is not required. It is important to note that this is in addition to clause 91 (2)

which authorises the Central government, in consultation with the Authority, to direct any data fiduciary to process anonymised personal data and non-personal data for the well-being of digital economy, targeted service delivery and so on. In matters relating to the breach of personal data, clause 25(5) confers discretionary powers on the DPA to determine whether or not a data principal has to be informed of the breach, depending on the basis of "severity" of harm. The denial of the autonomy of data principal to determine something as subjective as "severity of harm" of the data breach would impact the relationship between data principal and other entities. Furthermore, according to clause 83(2) a data principal cannot go to court, except in cases of complaint made by the authority. This denies a Data principal the right to be heard and seek effective redressal for the breach.

The PDPB also creates categories like biometric data, genetic data, personal data, sensitive personal data, non-personal data, critical personal data and anonymised personal data. Some of these categories may overlap (e.g. behavioural characteristics) and are difficult to operationalize in practice, providing leeway to and encouraging arbitrary practices from data fiduciaries. Instead, in accordance with the objectives of the Bill, an effort should be made to enable data protection and data minimisation rather than proliferation of control afforded by the creation of multiple categories. The PDPB under Clause26 not only distinguishes between data fiduciaries and significant data fiduciaries but also creates further obligations for significant data fiduciaries leaving data fiduciaries out of this purview. With changing technological advancements and increased usage of varied categories of data, such obligations need to be mandated for all kinds of data fiduciaries.

5. Discretionary powers of the Central government.

The Central government has been given enormous power under the PDPB. In practise the government has the power to operationalize the Act, however according to this Bill, the Central government is empowered to fix different dates for operationalization of different provisions of the Bill. Delaying operationalization of provisions containing safeguards can have serious implications on fundamental rights and liberties of the data principal. Moreover, such implications have critical consequences when the Central government exercises more discretionary power in framing policies for the digital economy. Clause 91(2) elucidates on the Central government's power to direct any data fiduciary or data processor to provide with any "personal data anonymised or other non-personal data" for the purpose of better delivery of services or for the formulation of any evidence-based policy. This particular clauseis indicative of the possibility of an arbitrary demand of non-personal data by the government besides inducing more uncertainty owing to the unclear definition of 'non -personal data' in the Bill. Additionally, Critical personal data should be defined in the Bill and not left to be deliberated upon later. Secondly, the Statealso under Clause3(27) has been defined as a "person" besides being the biggest data fiduciary. In such a

scenario, provisions such as Clause 28(2) stating that provisions contained in the said clause applies to the State as well notwithstanding anything contained in this Act may imply that rest of the provisions may not be applicable to the State. Therefore, it may appropriate to delete the said clause. It must be made clear that all the provisions of the Bill applies to the State as well unless otherwise explicitly provided. Lastly, since the State is a data fiduciary, DPA needs to be independent and have functional autonomyas recommended by the Srikrishna Committee.

On the whole, the PDPB, in its current avatar, lacks coherence and robustness to protect and safeguard the right to privacy and, thus, needs to be revised and brought in conformity the law laid down by the Supreme Court in K.S. Puttaswamy and also recommendations of Justice A. P. Shah and Justice Srikrishna Commissions.