The Personal Data Protection Bill, 2018 – Issues, Possible Solutions, and Recommendations

Raj Pagariya
Abhay Singh Sengar
Titiksha Seth
Sahana Chaudhuri

Contents

Acronyms/Referred to as

Name	Acronym/Referred to as
The Personal Data Protection Bill, 2018	The bill
A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians (Committee of Experts under the Chairmanship of Justice BN Srikrishna)	The report
White Paper of the Committee of Experts on a Data Protection Framework for India	The White Paper
European Union's General Data Protection Regulation	GDPR
The Data Protection Act 2018 (United Kingdom)	UK DPA 2018
The Information Privacy Act, 2014 (Australian Capital Territory, Australia)	Australia's ACT IPA 2014
The Personal Data Protection Act, 2010 (Malaysia)	Malaysian PDPA 2010
The Personal Data Protection Act, 2012 (Singapore)	Singapore PDPA 2012
Adjudicating Officer	AO
Reserve Bank of India	RBI
The Privacy Act, 1988 (Australia)	APA 1988
The Personal Information Protection and Electronic Documents Act, 2000 (Canada)	PIPEDA 2000
The Privacy Act, 1993 (New Zealand)	NZPA 1993

1. Right to be Forgotten u/s 27

Issue 1: Scope of the Right

The scope of the right given under Section 27 of the bill is limited only to restriction or prevention of a disclosure of a data principal's data by a data fiduciary. This right can be availed when such disclosure has –

(a) Either served the purpose or it is no longer necessary
(b) Consent given under Section 12 has been withdrawn
(c) Disclosure made in the contravention of existing laws

In addition, clause (2) of Section 27 states that for availing this right, it must override the right to freedom of speech and expression and the right to information of any citizen.

Prima facie, the scope under this section does not cover the deletion or erasure of a data principal's data stored by a data fiduciary. Comparing this right with similar rights given under various national and international regimes, the scope of this right must be widened. Though this right has gained prominence only in the last decade or so, it is equated with the Right to Erasure.

As per Article 17 (Right to Erasure – 'right to be forgotten') of GDPR, the grounds for availing this right are more or less same, but the extent is not. Article 17 of GDPR states that a data subject has a right to erasure of personal data concerning him or her without undue delay and the controller has an obligation to erase the personal data of a data subject on the basis of mentioned grounds. Similarly, The UK DPA 2018 has recognized the same right under its Schedule 6.

The question of whether an individual has a right to be forgotten which includes erasure of data has been brought up before the Indian Courts as well. Such courts include the High Courts of Gujarat, Delhi, and Karnataka. In February 2017, the Karnataka High Court recognised the right to be forgotten for removal of the petitioner's name from various case reports publicly available results via search engines.[1] According to the Justice Anand Byrareddy who presided over this case, this right can be availed in cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."

Since the bill recognises various rights of data principals with respect to their data and privacy, the right given under Section 27 shall also incorporate the right to erasure/deletion of data.

Possible Solutions

1. Appropriate modifications can be made in the present Section 27 of the bill by including words such as *deletion* and *erasure*. Along with this, additional grounds or restrictions can be added under Section 27(1) for availing this right.
2. An altogether different section can be added under Chapter VI of the bill for erasure or deletion of data. This section should cover situations where personal videos of victims are uploaded on online platforms without their consent *i.e.* revenge pornography cases. Misuse of such a right can

[1] https://cyberblogindia.in/right-to-be-forgotten-surfaces-india/

be prevented by narrowing the scope of the right using the Balancing principle, as discussed in Chapter 5 of the report.

3. Right to erasure can also work as a right to be deidentified from the information stored with a data fiduciary. "Deidentification" has been defined by Section 18 of Australia's ACT IPA 2014 which is on the similar lines as the definition of "anonymisation" given under Section 3(2) of the bill.

Issue 2 – Procedure for Exercising the Right

As per clause (4) of Section 27, a data principle can exercise his or her right to be forgotten by filing an application with the Adjudicating Officer. For the other rights given under Chapter VI of the bill, Section 28 lays down the procedure for exercising those rights by making a request in writing to the concerned data fiduciary. This procedure for exercising the right to be forgotten by stating that the data fiduciaries will be burdened with content removal requests and their decision will be biased towards their own interests. Further, the Committee stated that a data fiduciary is not capable of deciding between the statutory right to be forgotten and the fundamental rights to free speech and information.

Taking into consideration that an Adjudicating Officer (AO) is designated for each state at its capital, the pendency of cases can very well be inferred from the existing judicial system. On the other hand, India has a number of states covering vast geographical areas. For a data principal to appear at each hearing on his application, travelling costs and other practical factors may demotivate a data principal and result in losing the trust in the legal setup prescribed by the bill.

Or for a body corporate having its registered office in Mumbai, the same factors will come into play if they are called to appear before any Adjudicating Officer of the north-eastern states.

Possible Solutions

1. Just like other rights given under Chapter VI of the bill, the data fiduciaries shall be given an opportunity to erase or delete the data of a data principal. If the interests of a data principal supersede the interests of a data fiduciary in continuing to store it, the data must be deleted. For restrictions on the right to erasure, Recitals 65, 66, and 73 of the GDPR along with Section 35 & 36 of Malaysian PDPA 2010 can be referred to.
2. A statutory time limit of up to 30 days must be prescribed for dealing with such a request. A similar time-limit of 36 hours has also been prescribed under Rule 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011.
3. If a request for erasure or deletion of data is received or an order from an Adjudicating Officer has been received regarding the same, it must be the duty of a data fiduciary to inform all other data fiduciaries/processors with whom the data was shared. This duty has been recognised by Section 48 of UK DPA 2018 which further adds an obligation to inform all the recipients *i.e.* all the parties with whom data fiduciary had shared the data to erase it. A similar obligation has also been enforced under sub-clause (b) of Section 22(2) of the Singapore PDPA 2012.

4. If a data principal is not satisfied with the response given by a data fiduciary, he can follow the standard procedure of filing an application with the Adjudicating Officer.

A similar Standard Operating Procedure has been prescribed by the Reserve Bank of India in cases when there is no negligence on an account holder's end via its circular (Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI 2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18) dated July 06, 2017. As per the provisions of this circular, an account holder *i.e.* the victim has to first file an application with the concerned bank, and if there has been no response from the bank or the application is rejected, the account holder can approach the office of the Banking Ombudsman situated generally in a state's capital city.

2. Exemptions under the Bill

Issue 3 – No Exemption to the Armed Forces

Under Chapter IX, the bill grants exemptions to certain purposes which are laid down from Section 42 to 48. These exemptions include processing of personal data for –

- Security of the state
- Prevention, detection, investigation, and processing of contraventions of law
- Processing for legal proceedings
- Research, archiving or statistical purposes
- Personal or domestic purposes
- Journalistic purposes
- Manual processing by small entities

After going through various legislation enacted by the countries across the world, one can arrive at a conclusion that the armed forces of a country must be given a specific exemption under a data protection framework as the processes and procedures of the Armed Forces are altogether different from the procedure established by the law of the land for civil and criminal courts.

Section 70 of APA 1988, Section 7(3)(c.1) under Division I of PIPEDA, 2000, Section 23 of NZPA 1993, and Clause 7 Schedule 11 of UK DPA 2018 are some of the provisions of legislation across the world where Armed/Defense forces have been granted exemption from the national data protection framework in some way or the other.

Possible Solutions

1. A separate section under Chapter IX can be added for granting an exemption to Armed Forces, as done by the legislation mentioned above.
2. The exemption given under Section 42 of the bill *i.e.* Security of the State can be defined under Section 2 to include armed forces. For this definition, the definition of the phrase *national interest* given under Section 2 of Singapore PDPA, 2012 can be referred to. This phrase has been defined as

"*national interest includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs*."

3. Offences under the Bill

Issue 4 – Bailable & Non-bailable

Chapter XIII in the bill lays down various offences related to personal data of a data principal. This chapter also contains provisions when offences are done by either companies or Central/State government departments. After around 18 years of the enactment of the Information Technology Act, 2000, we have not been able to realize its potential due to non-consideration of the sensitivity of the harmed involved while classifying an offence as bailable and non-bailable. Here in the same chapter, Section 93 specifies that the offences defined in this act are cognizable and non-bailable without considering the sensitivity of the data.

Possible Solution

Whether an offence should be bailable or not should depend on the nature of the data affected. For offences involving sensitive personal data, the offences shall remain non-bailable while for the offences involving disclosure of personal data, the offences should be bailable.

Issue 5 – Power to Investigate

Another reason for non-realization of full potential of the Information Technology Act, 2000 is the power of investigation resting with a police officer, not below the rank of Inspector. The same status quo has been incorporated in the bill under Section 94. This section may be efficiently applicable in urban areas, while the same statement might not hold true for the police stations in suburban or rural areas as they are often headed by a police officer having the rank of Sub-Inspector. In addition, there is generally one police officer per police station having the rank of Inspector who is also designated as the station incharge while there are at least 2-3 subordinate officers having the rank of sub-inspector.

Possible Solution

The power to investigate for the offences given under the bill shall be given to a police officer, not below the rank of a sub-inspector.

4. Power and Functions of Authority

Issue 6 – Blanket Powers of DPA

Section 60 & 61 under Chapter X of the bill discusses various powers, functions, and responsibilities along with a prescription of standard Codes of Practice by the Data Protection Authority (DPA). These powers are given with respect to definitions of *processing* given u/s 3(32), *data fiduciary* given u/s 3(13), and *data principal* u/s 3(14). The provisions given under these sections give a blanket power to DPA to regulate the relationship between a data principal and data fiduciary.

As per the definition of data fiduciary, it can be any person including the State, a company, or any juristic entity or any individual who alone or in conjunction with others determines the purpose and

means of processing of personal data. This impliedly means that the number of data fiduciaries in the Indian cyber space will be substantially high. In order to balance between the interests of data principals as well as data fiduciaries, an independent board shall be set up to prescribe technical standards for activities defined under the definition of *processing* u/s 3(32).

Possible Solution

An independent board such as the Banking Codes and Standards Board of India (BCSBI) can be set up to lay down the technical standards for various processing activities defined under Section 3(32). The power given to DPA can be limited to enforcement of these standards and suggest appropriate changes to these standards to the said board. This board shall comprise of technical as well as legal experts having domain-specific knowledge in the activities given u/s 3(32).

5. Miscellaneous Recommendations and Suggestions

- The scope of the act given under Section 2 shall also include the data collected offline but processed or stored online.
- This bill is also silent on the aspect of ownership of personal data of a data principal. The bill must recognize data principal as the owner of his or her personal data.
- With possible technological advancements, it is possible that re-identification of a data principal is possible even after anonymisation of his data and hence, processing of anonymised data shall also be brought under the scope of this act by making changes in the definition of *personal data*.
- The definition of personal data u/s Section 2(29) does not specify whether it covers false information as well. Definition of personal data u/s 2 of Singapore PDPA, 2012 includes data about an individual whether true or not and hence, on the similar lines, the phrase *whether true or not* can be added to the definition in the bill.
- If a data principal exercises his rights given under Chapter VI, the concerned data fiduciaries shall also inform other fiduciaries with whom the data was shared.
- The notice framework given under Section 8 of the bill shall also include information such as –
    i. Whether data will be manually processed or automatically
    ii. Whether the collected data will be used for profiling or not
    iii. Whether the collected data will be used for direct marketing or not
- Majority of the debate on data protection in India is based on various reported incidents related to Aadhaar. Hence, UIDAI shall also be brought under the scope of this bill as a data fiduciary and power to enforce the provisions of the bill, as well as the remedies, shall be left to DPA and its adjudication wing.
- The definition of *harm* under Section 2(31) shall also include non-physical harms.
- Section 10 of the bill talks about limiting the storage limitation on the personal data of a data principal. In many cases, a data fiduciary may consider *reasonably necessary duration* to an extent which is highly beneficial in its favour. To prevent this, the duration for which personal data will be stored can be specifically mentioned in the notice under Section 8, subject to legal or regulatory requirements.

- For notification of a data fiduciary as a guardian data fiduciary, certain certification requirements must be prescribed and public opinion must be sought on this notification in order to cross-check the image of the said data fiduciary.
- Although the right to withdraw consent has been mentioned in the notice framework in Section 8 and Section 12(2)(e) considers a consent to be valid only if it is capable of being withdrawn, this right must be recognised as a separate right in Chapter VI so that a data principal has remedies available as per the procedure laid down by Section 28.

---x---