An Analysis of Personal Data Protection Bill, 2018

Dr. Vijeta Banwari, Assistant Professor, Maharaja Surajmal Institute

ABSTRACT

The Government of India constituted a committee of experts under the chairmanship of former Supreme Court Justice Shri B N Srikrishna in year 2017 to examine various issues relating to data protection in India and suggest a draft Data Protection Bill. This paper examines the key highlights of The Personal Data Protection Bill, 2018 and debate surrounding the issue by examining the opinion of corporate sector. The proposed bill applies to both government and private entities. The bill has drawn mix responses from the industry. Though the step of framing a law to ensure data privacy is welcomed by the industry but it is also criticized for some of its provisions. According to some stakeholders, legislation is contrary to the goals of promoting a Digital India: Data localization can hamper the growth of India's $135-billion software exports industry. Stringent data storage requirements lead to significant costs even for large companies, start-ups would be particularly affected by this measure. Start-ups are also concerned that the consent practices mandated under the Bill may be difficult to operationalise for certain technologies.

Key Words: Data Protection, Data Protection officer, data audit, data localisation

I Introduction

The Government of India constituted a committee of experts under the chairmanship of former Supreme Court Justice Shri B N Srikrishna in year 2017 to examine various issues relating to data protection in India and suggest a draft Data Protection Bill. After almost a year of consultation and deliberations with various stakeholders, the committee submitted its draft bill to the Ministry of Electronics and Information Technology (MeitY) on 27 July 2018. The bill lays down penalties, ranging from five crore rupees or 2% of total global turnover to fifteen crore rupees or 4% of the total global turnover. It is thus changing the way privacy is perceived and practiced within Indian business. (EY report 2018). The draft follows the implementation of the General Data Protection Regulation (GDPR) in Europe. It is said to have taken cues from the already present legal frameworks in different countries, such as GDPR in Europe, America's laissez-faire approach and The Chinese Cybersecurity Law, will surely feature the country on the world map. (Kulesh, Saurabh 2018)

According to the Bill, any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal. Personal data shall be processed only for purposes that are clear, specific and lawful. Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected. Also, collection of personal data shall be limited to such data that is necessary for the purposes of processing. (MEITY**, 2018)** Non-compliance with the Bill can attract penalties of up to Rs. 15 crores or 4% of worldwide turnover and even imprisonment up to five years.

The bill is a big step in protecting data privacy. However, the bill has drawn a mixed response from the industry and other stakeholders. According to critics, including data localisation requirements in such legislation is contrary to the goals of promoting Digital India, as global data transfers are critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. (Bhatia, 2018) Critics also argue that Data localisation may have a negative impact on long term innovation in India and hamper its growth.

In the light of above discussion, this paper examines the key highlights of The Personal Data Protection Bill, 2018 and debate surrounding the issue by examining the opinion of corporate sector.

II The Personal Data Protection Bill, 2018

The Draft of **Personal Data Protection Bill, 2018** is accompanied by its report titled *"A Free and Fair Digital Economy Protecting Privacy, Empowering Indians"* which provides context to the deliberations of the Committee. The processing of personal data is omnipresent in the public and private sector. Currently

norms relevant to data protection are spread across various statutes, which may lack overall consistency and general applicability. This creates ambiguity and irregularity in the protection of an individual's personal data. The proposed data protection framework must outline the minimum standards that will have to be followed and will have an impact on processing of personal data in all sectors, irrespective of more specific and overlapping sectoral statutes and regulations. (MeitY, 2018).

The proposed bill applies to both government and private entities. The applicability of the law will extend to data controllers/fiduciaries or data processors not present within the territory of India, if they carry out processing of personal data in connection with:

- Any business carried in India
- Systematic offering of good and services to data principles (also generally referred to as data subject) in India
- Any activity which involves profiling of data principals within the territory of India

The recommendations are as follows:

- The White Paper concluded that data portability should be included as a right so as to empower data principals to give them control over their personal data. Therefore, the White Paper argued that individuals should be able to access and transfer the data that they have provided in a machine-readable format.
- Regarding the right to object to direct marketing, the Committee has come to the conclusion that data fiduciaries may only engage in direct marketing based on consent of the data principal, which is freely given as per the reinforced standards of our framework. Therefore, if the data principal does not consent to a request to be solicited by direct marketing, a data fiduciary may not be allowed to approach the data principal with marketing material on any mode of communication. For consent to be valid it should be free, informed, specific, clear and capable of being withdrawn. For sensitive personal data, consent will have to be explicit.
- The data also proposes right to be forgotten i.e. ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.
- Data Localisation: Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government will determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement.
- For any processing activity of personal data inside or outside India, one "mirror copy" shall be required to be retained in India.
- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee.
- Employment and emergencies were accepted as Grounds for processing of personal data in addition to consent.
- Profiling, tracking or behavioral monitoring of or targeted advertising towards children (someone who is less than 18 years of age) is not permitted.
- Significant data fiduciaries will have to undertake obligations such as: (i) Registration with the Data Protection Authority (DPA) of India; (ii) Data Protection Impact Assessments; (iii) Recordkeeping; (iii) Data audits; and (iv) Appointment of Data Protection officer (DPO).
- Given that significant data fiduciaries may process considerably sensitive and large amounts of personal data, it is essential that they appoint a Data Protection officer (DPO) who facilitates compliance with data protection laws by monitoring and advising these fiduciaries as well as acts as a point of contact with the DPA. The eligibility and qualification requirements of the DPO will be specified by way of delegated legislation. The functions allocated to such DPO could include compliance monitoring, developing and ensuring robust compliance and accountability procedures, cooperating with the DPA, training staff, conducting DPIAs, grievance redressal, monitoring security safeguards, and maintaining records, etc. and notify PDA of any personal breach relating to personal data processed by it which can cause harm to a data principal. Failure to notify a breach will make the organisation liable to a penalty under the provisions of this law.

- Data audits should be undertaken by independent external auditors empanelled by the DPA to assess whether a significant data fiduciary's processing activities and policies are in compliance with the applicable data protection law.
- Organisations will need to retain personal data only as long as it is reasonably necessary to satisfy the purpose for which it is obtained. They will have to periodically review the personal data in their possession from a retention point of view.
- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.

III How will the Bill affect businesses?

Operationalising the privacy framework under the Bill will require companies to make significant changes to their data collection and processing practices. For example, companies will now need to take fresh consent from their users as per the detailed consent requirements under the Bill. Fintech and other companies will need to adopt higher security safeguards since a wide range of data is considered sensitive personal data. Companies will need to acquire the consent of their users in order to process their personal data. In order to be considered valid, consent needs to be free, informed, specific and capable of being withdrawn and indicated through affirmative action (so "pre-checked" consent boxes can longer be used). While seeking user consent, companies will have to provide users with detailed notices (on the basis of requirements under Section 8 of the Bill) at the time of collection of data. Additionally, companies cannot make the provision of any goods/services or their quality conditional on consent. Thus, access to websites or user registration cannot be conditional on consent, unless the data to be collected is necessary for the provision of such services. This can have impractical effects for the everyday use of publicly information like surnames that reveal caste/tribe or statements reflecting political/religious opinions available online – it appears that companies will need users' explicit consent for collection and use of even this freely available data. Data localisation may reduce access to global cloud service platforms for companies in India. It may also limit access to global markets and the latest technologies. This could cut into profit margins, reduce productivity for companies and undermine their competitiveness. (Ikigai Law, 2018).

What steps will Business have to take?

- Ensure data privacy and take accountability: Organisations will have to hold accountability of the personal data they own and ensure privacy of the same. Organisations will have to frame a mechanism for collection, storage of the data. They will have to give full disclosure of the information that they are collecting and take explicit approval from data principal. They may design an automated mechanism for collecting and storing such approvals. Update the digital presence: Organizations need to review their digital presence in line with the requirements of the bill- update their privacy statements, cookie policy, consent mechanism and online terms and conditions. Also, solutions will have to be implemented for management of cookies. (EY report, 2018)
- Provide rights to the data principal: The right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of information privacy. The data principal (natural person) will have the 'right to confirmation and access' and 'right to correction' of personal data. Further, the data principal will have the 'right to data portability' and 'right to be forgotten'. The biggest challenge which organisations face today is the multiple versions of the same data stored in different places and different systems such as ERP and CRM. This will require organisations to perform a massive data mapping exercise to understand the collection, storage, processing and transfer of information pertaining to individuals to support the data principal in exercising his rights. Organisations will have to prepare a brief summary of the personal data of the data principal being processed or that has been processed, and this summary will have to be updated and provided to the data principal. Organisations will have to invest in mechanisms and techniques to provide the data principal access to a copy of all the personal data they hold for correction or completion or update of inaccurate or incomplete personal data, thereby aiding data quality. Organisations will also have to take into consideration the data they provide to third parties for any legitimate business purpose. Also, it is imperative to record

all requests from data principals and track them to successful closure which means establishing the process, technology and structure to address such requests. Organisations will also have to acknowledge the receipt of requests from the data principal exercising any of the rights mentioned above within a reasonable time frame. Further, they will need to provide data principals the right to data portability, i.e. sharing of the data with other organisations or deletion of data upon request. (PwC report, 2018)

- Saving data locally: As per the Bill, organisations will have to store at least one mirror copy of the personal data locally. Further, critical personal data (as defined by Central government) will have to be stored locally. This has strong implications for the organisations as most of them have moved to cloud based infrastructure based outside India for storage and computing purposes. The organisations will have to identify alternatives to clouds based outside the country.
- Appoint a Data Protection officer (DPO) and register with DPA of India. Organisations will also have to be involved in Data Protection Impact Assessments.
- Report data breach to DPA without delay: Organisations will have to notify the Data Protection Authority (DPA) of any personal breach relating to personal data processed by it which can cause harm to a data principal. Failure to notify a breach will make the organisation liable to a penalty under the provisions of this law.
- Draft data retention policy organizations will have to draft retention policies highlighting the retention schedules (such as short term, standard and prolonged storage) for each data type collected and processed for data principals. The retention period needs to be drafted considering the legal, regulatory and business requirements. Policy should also be drafted for the backup and archived data. (EY report, 2018)

IV Responses from the Industry:

The bill has drawn mix responses from the industry. Though the step of framing a law to ensure data privacy is welcomed by the industry but it is also criticized for some of its provisions. They are discussed as follows:

1. According to some stakeholders, legislation is contrary to the goals of promoting a Digital India: According to industry, global data transfers are critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. Restrictions on data transfer will curtail the growth of businesses. It would increase cost of compliance for international tech giants like Facebook, Google operating in India. Data localization can hamper the growth of India's $135-billion software exports industry. (Bhatia, Richa 2018)
2. Permissions for the use of data will increase compliance formalities leading to reduction in efficiency.
3. Many startups place reliance on global cloud computing platforms such as Google Cloud, Microsoft Azure and Amazon's AWS. Their choice of cloud platforms is determined by the responsiveness of the service, cloud service latency, availability of disaster recovery centres and overall efficiency. Startups are concerned that data localization may not be immediately possible since improving the quality of cloud services in India will take enough time. According to startups, relying on servers located outside the country, may in fact be better for data security than storing all the data in one location, which can enable attacks. (Ikigai Law, 2018)
4. Need for guidance on how to operationalise notice and consent practices. Start-ups are concerned that the consent practices mandated under the Bill may be difficult to operationalise for certain technologies. Giving the example of facial recognition technology that is used to track and manage attendance of groups of students, a startup explained that while it is practicable to take consent on an individual basis, it would become extremely difficult to obtain the valid consent of larger groups of people in a crowd while capturing their faces. Startups using Internet of Things ("IoT") devices too may face issues providing notice and obtaining valid consent. IoT devices will need screens to display notices or will have to send emails in real time to users. This can come in the way of user experience and dissuade consumers from using these devices. (Ikigai Law, 2018)
5. Stringent data storage requirements lead to significant costs even for large companies, start-ups would be particularly affected by this measure. Boot-strapped startups operating under tight budgets

and resource constraints will be hit by the increased compliance costs entailed by the Bill. In order to facilitate compliance for smaller businesses, startups would like to see a carve-out for small businesses below a certain financial threshold– with relaxed standards for compliance being applied to such businesses. (Ikigai Law, 2018)

V Conclusion

The proposed bill has received mixed response from the industry. More guidance on implementation especially to start ups would help them in accepting it whole-heartedly. According to the bill, if India is to shape the global digital landscape in the 21st century, it must formulate a legal framework relating to personal data that can work as a template for the developing world. Implicit in such a belief is the recognition that the protection of personal data holds the key to empowerment, progress, and innovation. This bill will definitely reduce the cases of dat leakage, data misuse and will have long term positive effects.

References

- Bhatia, Richa. (JUL 30, 2018). Industry Verdict on Personal Data Protection Bill 2018: Noble Intentions, But Rocky Road Ahead. AnalyticsIndiamag. Retrieved on 20th December, 2018 from https://www.analyticsindiamag.com/industry-verdict-on-personal-data-protection-bill-2018-noble-intentions-but-rocky-road-ahead/
- EY (2018). Personal Data Protection Bill-2018-An initiative to enforce privacy principles in India. Retrieved on 20th December, 2018 from http://www.ey.com/Publication/vwLUAssets/ey-personal-data-protection-bill-2018/$File/ey-personal-data-protection-bill-2018.pdf
- Ikigai Law (17 October, 2018). Comments of certain start-ups on the Personal Data Protection Bill, 2018: Consolidated views. Retrieved on 20th December, 2018 from: https://www.ikigailaw.com/comments-of-certain-start-ups-on-the-draft-personal-data-protection-bill-2018-consolidated-views/
- Ikigai Law (2018). Draft Personal Data Protection Bill, 2018: what are the practical concerns? Retrieved on 20th December, 2018 from: https://www.ikigailaw.com/draft-personal-data-protection-bill-2018-what-are-the-practical-concerns/
- Kulesh, Sourabh. (Aug 04, 2018). Here's how India's Personal Data Protection Bill 2018 will affect you. Retrieved on 15th January, 2019 from: https://www.digit.in/internet/the-connection-between-personal-data-protection-bill-2018-and-an-indian-citizen-42611.html
- Ministry of Electronics and Information Technology (MEITY) (2018).The Personal Data Protection Bill, 2018. Retrieved on 25th December, 2018 from http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
- Ministry of Electronics and Information Technology (MEITY) (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians: Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. Retrieved on 10th January, 2019 from: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- PWC (2018). The Personal Data Protection Bill, 2018: What are the 10 things an organisation needs to do? Retrieved on 15th January, 2019 from: https://www.pwc.in/assets/pdfs/consulting/cyber-security/the-personal-data-protection-bill-2018.pdf