An Overview of the Draft Data Protection Bill, 2018

M.M.K. Sardana[*]

[***Abstract:*** *Data protection law refers to practices, safeguards, and binding rules put in place to protect one's personal information and ensure that one remains in control of it. In India, the data protection regime, as on date, is applicable to specific sectors. The all-encompassing reach of digital revolution requires a comprehensive law to address the concerns that are associated with the need of data protection and right to privacy of individuals while balancing it with the concerns of the state in meeting its duties of internal and external challenges. Further, data protection law has to pass the adequacy test of being in accordance with international law providing data safety. Government of India has with it a draft of the Personal Data Bill prepared by an expert group on which more than six hundred feedbacks have been received from stakeholders. This note examines the concepts enunciated in the draft Bill and offers comments on these concepts, particularly in regard to their implementation. It is recommended that the government should finalise its draft after weighing the inputs received and place the finalised draft in public domain to obtain further inputs before the draft is finally referred to the parliament for its consideration.*]

As one owns a smartphone, it is used for making calls, using internet, finding directions during travel, and opening a social media account. During all these uses of smartphone, one shares personal information, either online or offline, with private or public entities, including those that one may not have heard of. Using a smartphone and sharing of data may bring benefits, which are necessary given the everyday tasks and engagement with other people in today's society. However, it is not without risk. One's personal data reveals a lot about the individual, which may include one's thoughts and one's life. Such data can be used to harm the data subject and would be dangerous for vulnerable individuals and communities. This underscores the need for strictly protecting the data. In the European Union (EU), data protection is a fundamental right, and the General Data Protection Regulation (GDPR) is the framework for protecting this right. Many countries have looked up to GDPR and have either developed or are developing their own laws to protect data.[1]

A data protection law refers to practises, safeguards, and binding rules put in place to protect one's personal information and ensure that one remains in control of it, i.e. one should be able to decide whether or not one wants to share some

* The author is a Visiting Fellow at the Institute.

[1] Masse, E. (2018), "Data Protection Why it Matters and How to Protect it," *Access Now*, January 25. Available at: https://www.accessnow.org/data-protection-matters-protect/

information, who has access to it, for how long, for what reason, plus be able to modify some of this information, and more.

In India, there have been concerns about data protection. There are rules and regulations in place to address such concerns. Notable specific rules and regulations are:

1. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
2. Aadhar (Data Security) Regulation, 2016
3. Credit Information Companies Regulations, 2006
4. Telecom Commercial Communications Customer Preference Regulations, 2010
5. Clinical Establishments (Central Government) Rules, 2012

Thus, in India as on date, data protection regime is applicable to specific sectors with a target audience. The complexity, dynamism, and all-encompassing reach of digital revolution require a comprehensive regulatory regime to mitigate the concerns that are associated with the need for data protection.

A nine-judge bench of the Supreme Court of India in the case of Justice K.S. Puttaswamy (Retd.) vs Union of India & Ors held the right to privacy to be an intrinsic part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India. The Court, however, acknowledged that the right to privacy is not an absolute right and may be subject to reasonable restrictions by the State in proportion to the legitimate aims of the State.

State's duty is to protect national security and address internal and external challenges. Thus, the State may be required to have the ability to engage in real time surveillance of its data on need basis. The State may have to have access to data centres, including to the ones situated outside India.

India held 55 per cent of the share of the US$185–190 billion global outsourcing business during the Financial Year 2017–18. With the advent of GDPR w.e.f. May 25, 2018, transfer of data from the EU to non-EU country will need to pass the adequacy test and be in accordance with standard contractual clauses offering safeguards in relation to the data. It would thus be necessary for India to bring its own regulatory framework on data protection in line with the EU data protection framework.[2]

[2] Gupta, N. (2018), "India: Data Protection in India," *Mondaq*, October 10. Available at: http://www.mondaq.com/india/x/744160/Data+Protection+Privacy/Data+Protection+In+India

The need to address the shortcomings of the present data protection regime and the formulation of an omnibus data protection law, in line with the regulatory framework of international regimes, have come to the forefront. Government of India appointed a committee of experts under the chairmanship of Justice B.N. Srikrishna and entrusted it with the task of identifying the shortcomings in the present day Indian data protection laws and drafting a comprehensive data protection law for India. The Committee submitted its report along with a draft of the Personal Data Protection Bill. In its report, the Committee has made extensive references to the EU GDPR and many concepts of the GDPR have been reflected in the draft bill, suitably adopted to fit Indian data protection requirements.[3]

Recommendations made by the Srikrishna Committee stirred a debate among technology companies, startups, and industry bodies that are united in their stance for a law that should safeguard customers and help accelerate India's fast growing digital economy. India's primary IT (Information Technology) industry bodies such as National Association of Software and Services Companies (NASSCOM) and Data Security Council of India (DSCI) have been advocating for stringent data privacy and protection for years, especially since India is making rapid inroads into global digital market. Moreover, India's tech industry has become more inclined to respect and monitor data usage and storage ever since the Supreme Court ruled in favour of the right to privacy being deemed a fundamental right. Microsoft India has launched free online courses on data compliance basics of GDPR and other best practices in security. Indian banks and insurance companies have developed block chain infrastructure, which can safeguard customer data. There would emerge a rapid demand for skilled privacy professionals and specialists equipped to handle compliance requirements, which will flow from the Data Protection Bill as it is legislated and from the various privacy regulations across the world.[4]

Presently, the IT Rules, 2011, govern protection of personal data in India and are applicable to all body corporates. The draft Data Protection Bill, as presented by the Srikrishna Committee, seeks to address the lacunae in the IT Rules, 2011. It prescribes in detail the manner in which personal data shall be, *inter alia*, collected, processed, used, stored, and transferred, and applies to both government and private entities. The applicability of law is proposed to be extended to data

[3] Chakraborty, S. and A.R. Chowdhury (2019), "The Personal Data Protection Bill 2018: An Answer to India's Data Protection Issues?" *Business World*, January 01. Available at: http://www.businessworld.in/article/The-Personal-Data-Protection-Bill-2018-An-Answer-To-India-s-Data-Protection-Issues-/01-01-2019-165633/

[4] Balaji, S. (2018), "India Finally has a Data Privacy Framework: What Does it Mean for its Billion-Dollar Tech Industry?" *Forbes*, August 03. Available at: https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#68b04da470fe

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 goods and services to data principals/subjects in India
- Any activity which involves profiling of data principals (subjects) in India

This implies that the proposed bill seeks to have extra-territorial application and imposes compliance obligations for foreign data fiduciaries and data processors, even if they have an insignificant commercial presence in India.

The draft Bill introduces the concept of "data principal" and "data fiduciary." The natural person whose personal data is collected is referred to as the "data principal" and the entity that determines the purpose or means of processing the data is called "data fiduciary" and includes state, corporate entities, and individuals.

The definition of "sensitive personal data" has been widened to include intersex status, caste, tribe, and religious beliefs, and entities possessing such data will find their compliance obligations enhanced as the Bill is enacted.

Under the draft Bill, data fiduciary is required to give notice to the data principal before collecting, processing and/or using the personal data of the data principal. The notice would include the purposes for which personal data is to be collected/processed, the categories of personal data being collected, the details of data protection officers, the right of data principal to withdraw the consent, and the procedure for such withdrawal.

Personal data may be processed with the consent of the data principal. The consent will be valid only if it is free, informed, specific, clear, and capable of being withdrawn.[5]

The requirement of taking consent for processing data is enshrined in the IT Rules, though not in such detail.

The draft Bill focuses on compliances which data fiduciaries would find cumbersome. Certain obligations on data fiduciaries such as the requirement of giving notice, obtaining consent, etc., may pose practical and logistical issues and compliance with these would mean additional administrative burden and costs. Social media

[5] Anand, P. and V. Luniya (2019), "Understanding the Personal Data Protection Bill, 2018 and Bracing for Impact," *Live Law*, January 11. Available at: https://www.livelaw.in/law-firms/understanding-the-personal-data-protection-bill-2018-and-bracing-for-impact-142034

platforms, e-commerce companies, etc., have a wide user base spread across the country and obtaining their consent from the data principals in local languages would be a challenge.

The draft Bill proposes that the data fiduciary shall retain personal data only as long as it may be reasonably necessary to satisfy the purpose for which it is processed, unless required to be retained for a longer period of time mandated by law. The data fiduciary shall have to undergo annual audit compliance by an independent data auditor. Thus, the data fiduciary would be obliged to maintain accurate records. Similar provisions are there in the existing IT Rules as well.

Data fiduciaries, under the draft Bill, would be required to appoint Data Protection Officers (DPO) whose eligibility and qualifications would be prescribed under the rules. A DPO would be responsible for resolving the grievances within 30 days from the date of receipt from a data principal.

The Bill envisages creation of a central regulatory and adjudicatory body, i.e. DPA (Data Protection Authority), to enforce its provisions. The DPA would: (i) prescribe standards for the implementation of the provisions of the bill, (ii) function as a supervisory body, enforcement agency, and adjudicatory body, (iii) have extensive powers including that of suspending the business and activities of a data fiduciary or data processor if these are in contravention to the provisions of the Bill, and (iv) have power to conduct searches and seizures and of suspending or discontinuing the cross border flow of data. Thus, the powers proposed to be vested with DPA are very wide and discriminatory.

The present IT rules do not have provisions corresponding to DPA. The draft Bill recognises a class of data controllers called significant data fiduciaries who are subject to registration and have additional compliances to fulfil. Significant data fiduciaries would be notified by DPA based on factors such as sensitivity of data, volume of data processed, annual turnover, and risks involved. The thresholds for such factors are not provided in the bill leaving an ambiguity on the issue. At present, there is no equivalent concept in the existing IT Rules.

The draft Bill mandates data fiduciaries to ensure storage on a server located in India, of at least one copy of personal data to which it applies. The draft Bill specifies conditions under which data transfers outside the country may take place. Data localisation requirements would entail additional costs for setting up local servers in India. The obligation would have to be undertaken even when a foreign entity does not have a presence in India but where the provisions of the bill are applicable to such an organisation. With the exception of certain exempted categories, all entities, irrespective of the size or scale of processing, would need to comply with measures

such as privacy by design, security standards-encryption and de-identification, breach notifications, and transparency obligation.

Cross border transfer of personal data would be allowed in certain cases like: (i) transfer is to be made in execution of standard contractual clauses or intra-group schemes approved by DPA, (ii) where the central government, in consultation with DPA, has prescribed the transfer of personal data permissible to a country, or to a sector within a country or to international organisations, and (iii) transfer due to a situation of necessity approved by DPA.

The presently applicable IT rules do not define cross border transfer of data and data localisation. However, these rules prescribe that a body corporate, under its contractual obligation, may transfer sensitive personal data to any other body corporate or a person in India, or located abroad, that ensures the same level of data protection as is adhered to by the body corporates as provided under the IT rules.

The draft Bill proposes stringent penalties for contravention of its provisions ranging from Rs 5 crore to Rs 15 crore or 2 per cent to 4 per cent of an entity's total worldwide turnover, whichever is higher. Besides, a data principal can seek compensation from a data fiduciary, which will be over and above any penalties imposed. Such stringent penalties are not available under the present IT Rules.[6]

The draft Bill allows the processing of personal data in the interests of the security of the State if authorised and according to the procedure established by law. Access to all personal data by the state poses a threat to the right to privacy given the weak safeguards that exist in India against state surveillance. In combination with the data localisation requirement, the Indian government will have unlimited access to datasets that contain information about citizens.[7]

The draft Bill creates a regulatory structure that is not sufficiently independent. The Bill gives powers to the central government to not only appoint members of DPA, but also, if need be, remove them for specified reasons. India has a small pool of experts to match the qualifications required for being a member of the DPA. A revolving door is likely to be established between the regulator and data fiduciaries being regulated.

The draft Bill provided by the Srikrishna Committee has its share of positives, but at the same time, it is ambiguous in certain parts. Soon after it was received by the government, it was placed in public domain to elicit the views of both the general

[6] *Ibid*.

[7] CFR (2018), "Three Problems with India's Draft Data Protection Bill," Council on Foreign Relations, October 03. Available at: https://www.cfr.org/blog/three-problems-indias-draft-data-protection-bill

public and the stakeholders. Many experts and industry groups have responded and made their comments available to the government. The provisions of the draft Bill have been widely commented upon in the media also. In all, the draft Bill has attracted 600 sets of feedback, including from the US government. Multiple changes vetted in the bill have been incorporated in a draft finalised by the Ministry of Electronics and Information Technology (MeitY).[8] The government proposes to introduce the Bill for enactment in parliament in June 2019. There is thus an opportunity available with the government to place the finalised draft in the public domain and seek further inputs from the stakeholders, before it is readied and placed before the parliament for its consideration.

[8] F.R., Martin (2019), "India's Data Protection Bill Will Now Be Tabled in June," *Analytics India*, January 04. Available at: https://www.analyticsindiamag.com/indias-data-protection-bill-in-june/