An introductory analysis of the Joint Parliamentary Committee's report on Personal Data Protection Bill, 2019

March 2022

By Mayuran Palanisamy, Partner & National Lead (Data Privacy)—Digital Trust, KPMG in India and Jignesh Oza, Partner—Digital Trust, KPMG in India

(7 min read)

Key takeaways:

- *The industry can look forward to an integrated data protection regulatory framework with the primary objective of balancing individual privacy and innovation*

The Joint Parliamentary Committee (JPC)'s report has indicated that the government intends to have a command-and-control model of legislation to regulate an ever-evolving technology landscape. The Personal Data Protection Bill (PDPB) 2019 and the subsequent recommendations interpret data (including that derived from anonymised personal data) as a national asset to be exploited while balancing the rights of the individual. This is a marked departure from the European Union's General Data Protection Regulation's (GDPR) rights-based approach.

As per the latest information available on government platforms, India has the third largest startup ecosystem in the world[1], expected to witness a consistent annual growth of 12-15 per cent. As of 2018, of the 50,000 startups, 8,900 to 9,300 are technology led. 2019 alone saw an addition of 1,300 new tech startups[2]. With over 700 million internet users and 600 million smartphone users[3], India's digital economy needs a gentle yet firm regulatory hand in steering the innovation-fueled digital economy. The recommendations expressed by the committee allow room for cautious optimism by balancing the industry's need to access data sets against an individual's fundamental right to privacy.

In the year 2021, the government of India has issued an ancillary set of regulations governing social media platforms and intermediaries. Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, require 'publishers' to, among other things, append declarations of compliance in the terms and conditions or privacy policy displayed on their website. Businesses are, therefore, required to develop robust interconnected frameworks for compliance with the information security and privacy laws.

Key recommendations:

The JPC has made a total of 93 recommendations while proposing a 24-month window for compliance with the law. Certain key recommendations are outlined below.

- **Data protection bill and inclusion of non-personal data**
  To have a uniform regulatory structure for governing both personal and non-personal data, the JPC has recommended that the Data Protection Authority (DPA) be given additional jurisdiction to regulate processing of non-personal data too along with recommended regulations for its governance. Both will be formulated and included within the same bill. The JPC have, therefore, recommended that the erstwhile PDPB 2019 be retitled as the Data Protection Bill.
  By proposing a single law to govern both personal and non-personal data, the JPC has clearly indicated that the data frameworks to be created under the Bill would favour innovation and aim at creating a seamless flow of data and insights across public and private stakeholders. Since the regulations governing non-personal data are yet to be published, the additional burden for securing and lawfully processing personal data is difficult to quantify, as of date.

- **Data localisation**
  The JPC has chosen a stricter approach to data localisation by recommending that all the data involving Indian citizens be kept within the territorial limits of the country.

  With the 2022 Union Budget conferring status of 'infrastructure' to data centres, this sector is set to see a massive investment rush in the coming period[4]. This investment is expected to create a strong architecture for cloud-based innovations.

- **Reporting of personal data breach to data principal**
  The JPC has recommended removal of the 'significant harm' threshold and instituted a 72-hour deadline for intimating data principals of a breach. This implies that the erstwhile discretion available with data fiduciaries for reporting, has been withdrawn. Systems and processes must be fine-tuned to meet the deadline and avoid heavy penalties. Data fiduciaries will need to adopt a preventive rather than mitigatory approach. Investing in training and awareness programs in addition to upgrading their technical security measures is expected hold them in good stead.

- **Over the top platforms (OTT platforms) and social media**
  The JPC has recommended a complete overhaul in the way social media intermediaries and OTT platforms are regulated. Recognising and adopting the word 'platform' instead of 'intermediary', the JPC has recommended that these platforms take greater accountability for their processing and be responsible for verifying the identity of their users by using protocols like the 'know your customer (KYC) norms in other industries. Two other recommendations include regulating content published on their platforms through a newly formed social media regulator along the lines of the Press Trust of India and having a place of business in India.

- **Rights of data principal to be balanced with interests of state and data fiduciary**
  The right to be forgotten and the right to portability have been strengthened by increasing their scope and setting higher thresholds for rejection. This guideline, however, has been balanced by the recommendation of the right to erasure being considered with the government and the data fiduciary's interest. It is also recommended that the DPA issues guidelines for conditions of rejection.

- **Data protection officer (DPO)**
  The JPC recommends that the DPO should be a key managerial personnel (KMP) in a company. KMP are defined as CEO or MD or manager, whole time director, CFO, Company Secretary, or other personnel prescribed by law. DPO as a KMP may lead to higher accountability and increased efficiency due to direct oversight by the top management of the company.

- **Hardware manufacturers as data fiduciaries**
  The Ministry of Electronics and Information Technology (MeitY) warrants that all information technology (IT) hardware device manufacturers undertake a 'device evaluation'. The JPC has recommended an additional set of regulations to be formulated by the DPA along with certification standards formulated by the government. With three different agencies (MIETY, DPA and Certifying Authority) regulating a single commodity, attaining harmony between the regulations would be paramount for the sector's sustained growth.

- **Processing of personal data and sensitive personal data of children**
  The JPC has recommended that data fiduciaries processing children's data should ensure that they obtain consent from guardians and from children themselves three months before they turn 18 years old. It has also recommended that the distinction between data fiduciaries and guardian data fiduciaries be removed. This recommendation effectively places a higher obligation on all data fiduciaries to implement special controls by obtaining guardian consent, track it to maturity (18 years) and revalidate with the data principal.

Conclusion and way forward:

The recommendations issued by the JPC on PDPB 2019 allows room for cautious optimism. India needs a nuanced and holistic regulatory approach to balance the individual's right to privacy while sustaining the country's data-driven economic growth.

Organisations are well advised to assess their 'readiness' against the PDPB (revised to Data Protection Bill as per JPC recommendation) by taking stock of their personal data processing activities. Designing and developing privacy control frameworks covering privacy governance, data management, cross-border data flows, privacy by design and default domains are expected to translate into significant gains at the compliance stage. It is further posited that the PDPB is a step up from the existing Information Technology Act 200 (as amended) and all its regulations including IT (Reasonable Security Practices and Sensitive Personal Information) Rules 2011. The PDPB provides a more structured and nuanced approach for collection and processing of personal data and considered in instrumental in operationalising the fundamental Right to Privacy, in letter and spirit and aims ensure data sustainability for Digital India.

[1] Startup India website, Government of India, accessed on 21 February 2022

[2] Startup India website, Government of India, accessed on 21 February 2022

[3] India's growing data usage, smartphone adoption to boost Digital India initiatives: Top bureaucrat, The Economic Times, 26 October 2021

[4] Budget 2022: 'Infra status to data centers may spur Rs 70,000-72,000 crore investments over five-ten years, 1 February 2022