**ITU-APT Foundation of India**

**Submission to Joint Parliamentary Committee**

**Personal Data Protection Bill, 2019**

In 2017, the Supreme Court of India, in its landmark decision, *(Retd.) Justice K. Puttaswamy* v. *Union of India*[[1]](#footnote-1)(**Privacy Case**), upheld the right to privacy as a fundamental right under the Constitution of India. In 2018, an expert committee chaired by (Retd.) Justice B. N. Srikrishna set up by the Ministry of Electronics and Information Technology’s (**MEITY**) came up with a draft data protection bill. While the draft bill was submitted to the MEITY in July 2018 (**Srikrishna Bill**), a revised version of the Srikrishna Bill, the Personal Data Protection Bill, 2019 (**DP Bill**) was introduced in the Parliament during the winter session of 2019 and subsequently referred to a Joint Parliamentary Committee (**Committee**)for further review.

Given that the digital economy relies heavily on data of all types, any legislation to this effect must incorporate all principles of the Privacy Case as well as address the needs of the industry so as to ensure a robust and effective framework. ITU-APT Foundation of India aims to contribute to research, studies, and outreach in technical, regulatory, and other related matters affecting the sectors of telecommunications, broadcasting, and information technology. We appreciate the opportunity to participate in the dialogue between stakeholders commend the Government’s commitment to develop policy through a transparent and open consultation process. In light of this, the ITU-APT Foundation of India would like to take this opportunity to present its views on the DP Bill before this Committee.

1. **Grounds of Processing**

Apart from consent, the DP Bill recognizes other grounds of processing such as functions of the state, compliance with law or any order of any court or tribunal, prompt action, employment and reasonable purposes. Given the volume and nature of data that is collected from data principals on a daily basis, the DP Bill fails to include sufficient grounds for processing personal data. For example, while the European Union General Data Protection Regulation (**GDPR**) provides for contractual necessity as a ground for processing, the DP Bill has no such mention. The DP Bill does not consider, as a lawful basis, the processing of personal data to fulfil contractual obligations. This not only creates additional layers of consent required to be obtained from data principals even after the data principal has provided his/her consent to the contract, it also leads to consent fatigue.

Though the Data Protection Authority (**DPA**) is empowered to notify “reasonable purposes” for which data may be processed, data fiduciaries should also be permitted to determine alternate grounds based on certain principles. This list of “reasonable purposes” is limited and can only be determined by the DPA. The grounds of processing for sensitive data are even more limited.

The DP Bill should allow for processing on wider grounds so as to ensure constant functioning of the digital economy, which may otherwise be disrupted due to ongoing compliance requirements that are not practicable.

1. **New Categories of Fiduciaries**

The DP Bill introduces several new elements including a category of fiduciaries known as “social media intermediaries.” It is not clear why such a separate category is introduced. It is manifestly arbitrary and there is a strong constitutional argument for striking down such an unreasoned classification. It is also not clear why such categories of data fiduciaries, when they are classified as “significant data fiduciaries” will need to enable identity verification of users. This is quite antithetical to privacy and should be reconsidered.

1. **Data Protection Authority**

The DPA plays a crucial role in the enforcement and implementation of the DP Bill. It enjoys several legislative, administrative, and quasi-judicial functions, therefore, as an independent regulator, the DPA must be set up so as to ensure that the objectives of the DP Bill are adequately met.

1. *Selection Committee*

The composition of the Selection Committee, which shall appoint members to the DPA has been amended to consist of members from the Central Government only. Though the Srikrishna Bill had recommended the composition of the Selection Committee to include experts and judicial members, the current provision includes civil servants only. This composition may undermine checks and balances given that the representation will be restricted to just the Central Government. Therefore, the composition as suggested in the Srikrishna Bill should be retained.

1. *Financial Independence*

The DPA derives its financial resources from the Central Government, which again raises questions regarding the financial independence the DPA. Since receiving funds from the Central Government may pose risks of undue political influence, as an independent regulator, the DPA must be financially autonomous so as to ensure that its unbiased functioning.

1. **Data Portability**

The definition of personal data now includes inferred data – an expansion which should be resisted on account of multifarious implications. This changes implication of the right to data portability in the DP Bill is with respect to the types of data that can be transferred from one service provider to another. The DP Bill allows provides the right to data portability for (a) data provided by the data principal to the data fiduciary; (b) data which has been generated in the course of provision of services or use of goods by the data fiduciary; and (c) data which forms part of any profile on the data principal or which the data fiduciary has otherwise obtained. This would mean that any data that is inferred or derived by the data fiduciary is also portable. Since such data which is inferred or derived is a result of the deployment of tools by the data fiduciary, such datasets would be likely to be proprietary information. Since data portability enables data principals to transfer their data, any transfer of such data between service providers may be an infringement of copyright law. Therefore, data portability should happen through industry led standards. In the alternate, it may include only data that has been directly provided by the data principal, and should not include any inferred or derived data.

1. **Data Localization and Cross-Border Transfer of Data**

In a data-driven economy such as India, free cross-border flow of data is essential for the growth of the sector. Any restrictions or conditions may impact the smooth functioning of the businesses operating worldwide and that depend on shared data. While the DP Bill has removed localization requirements for personal data, it continues to require sensitive personal data to be stored in India and critical personal data to be processed and stored in India. Any transfer of sensitive personal data and critical personal data are required to meet additional conditions including explicit consent and other criteria such as adequacy decision, approval of the intra-group scheme or contract from the DPA, etc.

Requiring companies to get approval from the DPA for their intra-group schemes, contracts or in specific cases would lead to administrative delays and would not be feasible for data fiduciaries and the DPA. An approach like in the GPDR where the authority would approve a set of model clauses should be adopted so as to avoid any inconvenience.

1. **Age-Gating**

The DP Bill restricts data fiduciaries from processing the personal data of minors and young adults (below the age of 18 years) that are availing any goods and services online. While the digital age of consent for data protection laws across the world is much lower, the age-gate of 18 years in the DP Bill fails to account for the knowledge and maturity in young adults who are empowered to decide how their data may be processed and reap significant benefits from the same. Requiring parental or guardian consent for each instance of data use will prevent businesses from offering its services to young adults owing to such high compliance and risk of liability. This may rob young adults from useful online tools, for example, e-learning services, which is currently catering to the learning needs of thousands of children who do not have access to formal schooling systems. Unnecessary restrictions for such services would further widen the knowledge gap in the country.

While it is important to protect children from harmful data or targeting activities, businesses should be allowed to determine how to offer their services and develop age-gating mechanisms suitable to their interface but subject to adhering to privacy and security safeguards. Instead of the State mandating an age-gate, entities should take all possible reasonable steps to ensure that data of young adults is used only for pro-consumer purposes.

1. **Non Personal Data**

The DP Bill makes a provision for the government to direct collection of non personal data from companies – loosely defined as any data that is not personal. This gives rise to concerns regarding expropriation of data assets, in addition to simply having no nexus with the objective of data protection. Such a provision could have severe negative implications for the digital economy and should be reconsidered.

1. **Penalties and Liability**

While the DP Bill has been amended with respect to certain offences, the DP Bill retains its approach to impose criminal liability as well as monetary penalties for contravention by data fiduciaries.

1. *Criminal Liability*

Imposing criminal liability on the people in charge of the data fiduciary’s business for any contravention of the DP Bill is harsh and excessive. Since alternative approaches are available, imprisonment of individuals for contravention will only prevent companies from investing in India owing to such a harsh liability regime.

1. *Monetary Fines*

Similarly, imposing monetary penalties on data fiduciaries for contraventions and basing such penalties on the worldwide turnover of the data fiduciary will further discourage companies from targeting Indian markets. This will, in turn, affect investments and stifle innovation.

Given that harsh monetary penalties are not ideal, the DP Bill should only impose them as a last resort measure, and limit the scope of such fine. Instead of such harsh fines, the DPA should align its practices for enforcement to international standards so as to prevent any potential harm. For example, enhanced tools for detecting breaches may prevent any unlawful disclosure of personal data.

1. **State Exemption**

The DP Bill contains expansive exemptions for state actors from the purview of the provisions of the DP Bill. Such a blanket exemption is problematic as it is does not meet the requirements of legality, necessity, and proportionality as upheld in the Privacy Case. Any exemption given to the State must be reconsidered to include adequate safeguards and prevent any misuse or abuse of State power, for example, State-sanctioned surveillance.

1. **Transition Period**

While the Srikrishna Bill contained an entire chapter on transition provisions which set out timelines for the periodic implementation of the different provisions of the legislations, the chapter has been deleted from the DP Bill. It is pertinent to note that in the case of the GDPR, the entire digital ecosystem was given a period of 2 years to align its practices and policies with the new requirements of the GDPR. Given that the DP Bill overhauls the current regime with additional compliance requirements, the DP Bill must include specific transition provisions so as to provide data fiduciaries and processors sufficient time to change their privacy and security policies and align it with the requirements prescribed by the DP Bill.

1. (2017) 10 SCC 1 [↑](#footnote-ref-1)