Summary and Primer on Joint Parliamentary Committee Report and Data Protection Bill, 2021

The Joint Parliamentary Committee chaired by Member of Parliament Shri P.P. Chaudhary tabled the report[1] on the Data Protection Bill before both houses of parliament on the 16th of December 2021. The document comprises two parts, the first half of which is the report, and the second is the amended Bill. The Committee deliberated for over two years, during which time that Bill underwent substantial changes in scope and nature. A brief summary and primer to the report and the new highlights of the Bill are substantiated below.

Joint Parliamentary Committee Report Summary:

The Report submitted by the JPC highlights the country's digital priorities. Report states the need to balance the need for data-driven innovation while catering to national security demands. The Report defines the various data assets of the country and illustrates how they may be poised as instruments of economic advancement and refers to goals of AatmaNirbhar' Bharat and Make in India. The Report acknowledges that data protection is a universal concern, and meaningful legislation is imperative for a country to function in the global market. Therefore, it recognises the importance of cross-border compatibility in data protection legislation. To that end, it looks to contextualise the Bill through the global legal framework, especially through the lens of the EU GDPR[2]. The report emphasises the prime role of data in national security and recommends interventions that can be deployed to protect the data assets of the country. In many ways the report seems to set the context and offer a justification for the amendments sought to be made by the Committee, in the PDP Bill 2019.

Some key recommendations are as follows:

1. **The new legislation will deal with personal and non-personal data both:** The Committee have observed that to define and restrict the new legislation only to personal data protection or to name it as Personal Data Protection Bill is detrimental to privacy. Citing impossibility in discerning between Personal and Non-Personal Data, during mass collection and usage. In Committee's view, all the data has to be dealt with by one Data Protection Authority (DPA). **(Recommendation 1)**

2. **Government asked to follow a timeline for phased implementation of Data Protection Act:** Committee opined that absence of specific provisions for transitional phase necessarily creates uncertainty for the concerned stakeholders. The Committee, recommends that an approximate period of 24 months may be provided for implementation of any and all the provisions of the Act so that the data fiduciaries and data processors have enough time to make the necessary changes to their policies, infrastructure, processes etc. **(Recommendation 2)**

3. **Government asked to bring mirror copy of the sensitive and critical data from abroad and do localization.** Committee recommends that apart from provisions under Clause 33 and 34 for cross-border transfer of data, some concrete steps must be taken by the Government to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time bound manner. **(Recommendation 10)**
4. **Policy to be prepared and pronounced for Gradual data localization recommended.** Committee have specifically recommended that the Central Government, in consultation with all the sectoral regulators, must prepare and pronounce an extensive policy on data localisation encompassing broadly the aspects like development of adequate infrastructure for the safe storage of data of Indians which may generate employment; introduction of alternative payment systems to cover higher operational costs, inclusion of the system that can support local business entities and start-ups to comply with the data localisation provisions laid down under this legislation; promote investment, innovations and fair economic practices; proper taxation of data flow and creation of local Artificial Intelligence ecosystem to attract investment and to generate capital gains. **(Recommendation 11)**

[1] Access here.
[2] Regulation (EU) 2016/679 (General Data Protection Regulation)

5. **Government asked to establish a mechanism for certification of all digital and IOT devices.** Committee has strongly recommended that the Government should make efforts to establish a mechanism for the formal certification process for all digital and IoT devices that will ensure the integrity of all such devices with respect to data security. **(Recommendation 8)**

6. **Social media platforms to be treated as publishers and be regulated for the content they host.** Committee has recommended that all social media platforms, which do not act as intermediaries, should be treated as publishers and be held accountable for the content they host. A mechanism may be devised in which social media platforms, which do not act as intermediaries, will be held responsible for the content from unverified accounts on their platforms. **(Recommendation 5)**

7. **Reporting of Breach of personal data within specific time directed.** Committee has recommended a fixed timeline of 72 hours for breach reporting. **(Recommendation 38)**

Amendments to the Personal Data Protection Bill, 2019 to the new Data Protection Bill, 2021:

Highlighted below are some of the key changes in comparison to the 2019 draft of the legislation:

1. **Material scope of application**: The committee is of the opinion that for the purposes of this bill, privacy should be viewed in the context of information available in the digital domain alone. Hence, non-digitised data should not be governed under this bill. (Para 2.12)

2. **Non-Personal Data:** The Act brings both personal and non-personal data within its scope. The report highlights the primary reasons why non-personal data is brought into the purview of the legislation.
   - As the Bill is dealing with various kinds of data at different levels of security and it becomes impossible to distinguish between personal data and non-personal data when mass data is collected or transported.
   - Non-personal data is brought into the scope of the DPA as it will eventually have to deal with the broader ambit of data protection regardless of whether it is personal data or no-personal data.
   - The Committee has also noted that non-personal data is essentially derived from the anonymisation of personal data - sensitive personal data and critical personal data. And hence can be brought within the scope of the Data Protection Bill at large.

3. **Criminal Penalties**: The offences punishable under the scope of the Bill shall be cognizable and non-bailable. The criminal penalties include imprisonment of up to three years and a fine of two lakh rupees. The Data Protection Bill highlights that no court shall take cognisance of any offences punishable under the Act, save in the cases where a complaint is made in writing either by the Authority or an officer authorised for this purpose. The Bill also mentions that an "independent director and a non-executive director of a company shall be held liable only if it is shown that the acts of omission or commission by the company had occurred with his knowledge or with his consent attributable to him or where he had not acted diligently".

4. **Data Localisation:** Both the report and the Bill calls for continual storage of sensitive personal data in India and storage and processing of Critical Personal data only within the territory of India, transfer of critical data outside India is subject to DPA approval in consultation with government.

5. **Accountability and Transparency Practices:** Chapter 6 of the Data Protection Bill looks at the nature and scope of accountability and transparency for data collection and processing systems. The Bill overall places the responsibility of data protection and the transparency of processing activities squarely on the data fiduciaries and by osmosis on data processors, as mentioned in Clause 10 of the Bill. Such transparency is ensured by reporting a data breach within 72 hours of becoming aware of such an event occurring and calling for the appointments of Data Protection Officers. The revised Bill calls on the need for companies to implement Privacy by Design, especially in the cases of Fairness, Accountability, and Transparency (FAT) of algorithms. The report also highlights that one of the critical concerns for the Committee is

the transparency and accountability expected of social media intermediaries. To increase accountability of such platforms, the Committee opined that social media platforms that do not act like intermediaries should be considered publishers who control the content published on their platforms. The Committee also suggested that social media intermediaries should verify their users to increase accountability and should not be allowed to operate in India unless the parent company sets up an office within the territory of India. The Committee has further suggested that a statutory media regulatory authority - like the Press Council - should be set up to regulate content on such platforms.

6. **Timeline for Implementation:** A timeline for set-up, implementation and compliance has been specified within the Bill and the report. As it stands, companies are given a period of 24 months or 2 years to comply with the legislation once it comes into effect. However, there has been no mention of a separate or implicit timeline for data localisation requirements.
