client alert

December 19, 2021

cyril amarchand mangaldas
ahead of the curve

The Report of the Joint Parliamentary Committee on the Data Protection Bill, 2019: Curiouser and Curiouser

India has waited a long time for its general data protection legislation[1].

Since *Puttaswamy*[2], it has been evident that this key piece of legislation -- which will govern the data of over 1.4 billion people, impact businesses ranging from corner stores to the world's largest conglomerates, and create what may be the most powerful regulator in the nation -- had to be drafted with a deft hand and sustain a delicate balance.

The report of the Justice Srikrishna Committee[3], prepared after extensive consultations and with the avowed purpose of creating a free and fair data economy, was a strong step in this direction. It proposed a personal data protection bill[4], which while not without its rough spots[5], was an impressive attempt at developing a global data protection regime for Indian needs.

A version of the Bill, somewhat worse for the wear[6], was finally introduced in the Lok Sabha on December 11, 2019 as the Personal Data Protection Bill, 2019 ("**2019 Bill**")[7]. There were several concerns raised about this document, which was, in turn, referred to a Joint Parliamentary Committee ("**JPC**") for review.

This JPC, over its two-year tenure, had been extremely prominent and active, conducting multiple rounds of consultations with 78 sittings. During this time, the JPC got five extensions and saw a change in leadership in July 2021 when several of its key members were elevated to prominent ministerial positions.

The JPC's tenure coincided with very relevant developments including high profile data breaches[8] and geo-political developments[9], and it had the difficult task of fine tuning the 2019 Bill to find this delicate balance.

The eagerly awaited report was tabled before both houses of the Parliament on December 16, 2021 ("**Committee Report**")[10] and proposed nearly 90 drafting and 90 substantive changes in the 2019 Bill along with the draft of the Data Protection Bill, 2021 (**2021 Bill**).

1 The Group of Experts on Privacy, chaired by Justice AP Shah, postulated the need for this in their report titled 'Report of the Group of Experts on Privacy' dated October 16, 2012, available here.
2 *Justice KS Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 ("**Puttaswamy**").
3 Report of the Committee of Experts constituted under the Chairmanship of Justice Srikrishna (Retd.) titled 'A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians', available here.
4 The Personal Data Protection Bill, 2018 ("**2018 Bill**"), available here.
5 See our analysis of the 2018 Bill here, and its comparisons with the GDPR here.
6 See our analysis of the 2019 Bill here.
7 The Personal Data Protection Bill, 2019, available here.
8 News reports on some of the recent data breaches in India are available here and here.
9 Interesting developments in India during the JPC's tenure include the Government's ban on Chinese apps, available here and the Government's increasing push towards data localisation, available here and here. Further, several key developments in the privacy space at the international level occurred during this period, please see here.
10 Report of the Joint Committee on the Personal Data Protection Bill, 2019, available here.

The following is our analysis of some of the most important ones.

A. Non-Personal Data:

The most significant change proposed by the JPC by way of the 2021 Bill has been to include within its ambit non-personal data[11], which has been defined to mean "any data which is not personal data"[12].

While the broad concept, i.e. the Data Protection Authority ("**DPA**") will be best placed to regulate all matters relating to data (whether personal or non-personal) is probably preferable to creating a parallel regime[13], this approach creates two essential problems:

(i) ***A Negative Definition***: The 2021 Bill defines everything except personal data as "non-personal data" and requires the reporting of all non-personal data breaches, which include "accidental disclosure, acquisition or loss of access" to such "non-personal data"[14]. Read together, this may mean that the DPA is inundated with notices every time there is an outage at a datacenter.

(ii) ***Consolidating Disparate Categories***: The 2019 Bill was the outcome of *Puttaswamy*, which upheld and reaffirmed that privacy is a fundamental right. Non-personal data enjoys no such status, and indeed may never need to, as it may not relate to anyone. While much will depend on the rules prescribed by the DPA, attempting to regulate it in the same framework with personal data runs this risk of creating unnecessarily onerous obligations.

B. Timeline for Implementation:

Acknowledging the recommendations from the industry, the JPC has recommended a phased implementation of the 2021 Bill, giving due regard to the processes required to be set up, minimising business disruption and providing lead time for various stakeholders to establish compliance mechanism. The phased implementation timeline of the 2021 Bill, recommended by the JPC is: (i) 3 (three) months, for the appointment of Chairperson and Members of the DPA; (ii) 6 (six) months, for the DPA to commence its activities; (iii) 9 (nine) months, for registration of data fiduciaries to start; and (iv) a maximum period of 24 (twenty-four) months for the implementation of all the remaining provisions of the 2021 Bill[15]. Given the anaemic and poorly enforced current data protection regime, businesses may need time to overhaul their infrastructure and processes to comply with the demanding provisions of the 2021 Bill.

C. Transfer of Data to Third Parties:

The JPC has recommended inclusion of a new sub-Section 8(4), which restricts data fiduciaries from sharing or transferring any personal data with other data fiduciaries or processors, as a part of any business transaction, other than as permitted[16]. This change is confusing and potentially very problematic were it to be read to require fresh consents to be collected by each data fiduciary. Sharing personal data, based on valid consents, and in furtherance of the purposes for which such consent was accorded, is how business data flows occur, including under the European Unions' General Data Protection Regulation ("**GDPR**")[17].

D. Sensitive Personal Data and Cross-Border Transfers:

The JPC has recommended fairly stringent requirements for cross-border transfer of sensitive personal data. The proposed changes to Section 34 of the PDP Bill, specifically a *proviso* to Section 34(1)(a)[18], require that all intra-group schemes be approved by the DPA in consultation with the Central Government including ensuring that the object of such transfer does not violate public policy[19] or state policy. The object itself can vary from contract to contract and evaluating each, brings in an element of subjectivity while potentially taking away the possibility of prescribing a standard form of contractual clauses for such transfers. The need for a case by case approval, even *post facto*, may result in delays and significant business disruption. Further, granting such approvals based on the object of transfer will necessitate the analysis of specific transactions, which may result in the DPA -- an authority which is

11 Long Title, 2021 Bill.
12 Clause 3(28), 2021 Bill.
13 Revised Report of the Committee of Experts on Non-Personal Data Governance Framework, dated December 16, 2020, available here.
14 Clause 3(29) read with Clause 25, 2021 Bill.
15 Recommendation 3, Committee Report.
16 Clause 8(4), 2021 Bill.
17 General Data Protection Regulation (EU) 2016/679, available here.
18 Proviso to Clause 34(1)(a), 2021 Bill.
19 Explanation to Clause 34(1)(c) of the 2021 Bill defines 'Public policy' or 'State policy' to mean an act which promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizens.

already vested with substantial powers and burdened with significant oversight obligations -- being saddled with enormous workloads.

Additionally, the restriction on sharing transferred data with foreign government or agency[20] and the inclusion of Recommendation 11, which recommends bringing back a mirror copy of data stored outside India in a time-bound manner[21] may result in a *de facto* hard localisation requirement for sensitive personal data.

E. Social Media Intermediaries and Social Media Platforms:

The JPC in the Committee Report has noted the role of social media platforms in disseminating the content hosted by them with concern. The JPC noted that such social media platforms are designated as intermediaries and there isn't a strong mechanism under current law to hold them responsible for the content they publish despite their ability to determine the accessibility to such content[22]. It has requested the government to treat such social media platforms as publishers and for the purposes of the 2021 Bill has defined them as "platforms"[23]. Further, the JPC has recommended that they should be allowed to operate in India only if their parent entity sets up an office in India[24].

The 2021 Bill, in defining the social media platforms tracks the definition of social media intermediary in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Guidelines**")[25].

F. Definition of Harm:

The definition of harm has been expanded to include "*psychological manipulation which impairs the autonomy of the individual*"[26]. Given that the intent behind most targeted advertising and data analytical modelling is to influence individual behaviour, it would be interesting to see how harm is interpreted in the context of psychological impact.

G. Changes to the Consent Framework:

Changes have been made to the 2019 Bill to clarify ambiguous language and strengthen the requirement of obtaining explicit consent of data principals for processing of sensitive personal data without making any implicit inferences from conduct or context[27].

Further, the 2021 Bill includes a new sub-Section specifying that provision of goods and services to data principals may not be denied by a data fiduciary based on exercise of choice[28]. While the objective of the JPC to amend Section 11(4) seems to be clarificatory with the intent of restricting an entity from denying the provision of any goods or services conditional on consent to provide personal data that is not relevant to the service, the drafting of 11(4)(ii) ("*based on exercise of choice*") is ambiguous and has the impact of overriding Clause 11(4)(i) (*restriction on making the services conditional on data not relevant for the services*) and rendering it dead letter.

H. Exercise of Rights by Data Principals:

(i) ***Children***: The 2021 Bill extends restrictions on profiling, tracking, behaviour monitoring or targeted advertising that causes significant harm to children, to all data fiduciaries[29]. Further, data fiduciaries involved in processing children's data or providing services to them will be classified as significant data fiduciaries[30]. The Committee Report also recommends that data fiduciaries: (i) dealing exclusively with children's data to register themselves with the DPA; (ii) remind a child, 3 (three) months prior to attaining majority, to provide consent upon attaining 18 (eighteen) years of age; and (iii) continue to provide services till fresh consent is taken or such child opts out[31].

(ii) ***Death***: The JPC has recommended that data principals should be provided an option to nominate a legal heir and exercise the right to be forgotten in the event of death[32].

20 Clause 34(1)(b)(iii), 2021 Bill.
21 Recommendation 11, Committee Report.
22 Recommendation 6, Committee Report.
23 Recommendation 6, Committee Report.
24 Recommendation 6, Committee Report.
25 Rule 2(w), Intermediary Guidelines, available here.
26 Clause 3(23), 2021 Bill.
27 Clause 11(3)(b), 2021 Bill.
28 Clause 11(4), 2021 Bill.
29 Clause 16(4), 2021 Bill.
30 Clause 26(1)(g), 2021 Bill.
31 Recommendation 5, Committee Report.
32 Clause 17(4), 2021 Bill.

(iii) ***Right to Data Portability***: Data fiduciaries can no longer deny data portability on the grounds that it reveals a trade secret[33]. The right to refuse data portability has been limited to technical non-feasibility, as is determined by the data fiduciary in such manner as may be specified by regulations[34].

(iv) ***Transparency***: The JPC has recommended that data fiduciaries will need to provide information in relation to ensuring fairness of the algorithm or method used for processing of personal data[35]. This will impact businesses undertaking targeted advertisements, recommendations or any commercial or priority listings on search engines and may also force entities to reveal proprietary information regarding the functioning of their digital platforms.

I. Reporting of Data Breaches:

While the obligation to report certain data breaches was always part of the 2019 Bill, the 2021 Bill expands on the requirement. The 2021 Bill mandates data fiduciaries to report every incident of data breach involving personal data to the DPA, irrespective of whether it is likely to cause any harm to the data principal[36]. The 2021 Bill further adds that the form and manner of notifying the DPA will be specified by regulations[37], and such notice must be issued by the data fiduciary within 72 (seventy-two) hours of becoming aware of such breach[38]. Upon evaluating the nature of breach and severity of harm that may be caused to the data principal, the DPA may direct the data fiduciary to report such breach to the data principal and take appropriate remedial actions to mitigate such harm[39]. In relation to breach involving non-personal data, the DPA may take steps as necessary[40].

While not as part of the text of the 2021 Bill, the Committee Report sets out certain guiding principles[41]

that the DPA may follow while framing rules and regulations in relation to data breaches which *inter alia* requires data fiduciaries to maintain a log of all data breaches (involving both personal and non-personal data) and prove that the delay was reasonable in case a data principal suffers harm (whether material or immaterial) due to delay in reporting of a data breach.

J. Certification of Hardware and Software on Computing Devices:

The Committee Report envisages setting up a formal certification mechanism, through dedicated labs/ testing facilities for all digital and IoT devices, to ensure integrity of such devices in terms of data security[42]. Accordingly, it has added as one of the functions of the DPA, the monitoring, testing and certification by an appropriate agency authorized by the Central Government to ensure integrity and trustworthiness of hardware and software on computing devices to prevent any malicious insertion that may cause data breach[43].

33 Recommendation 40, Committee Report.
34 Clause 19(2)(b), 2021 Bill.
35 Clause 23(1)(h), 2021 Bill.
36 Clause 25(1), 2021 Bill.
37 Clause 25(2), 2021 Bill.
38 Clause 25(3), 2021 Bill.
39 Clause 25(5), 2021 Bill.
40 Clause 25(6), 2021 Bill.
41 Recommendation 4, Committee Report.
42 Recommendation 10, Committee Report.
43 Clause 49(2)(o), 2021 Bill.

While the JPC has proposed significant changes to the 2019 Bill, interventions such as specifying clearer reasonable purposes and clarifying the category of critical personal data would have been welcome. Much is still left to the Central Government and the DPA to clarify through formulation of rules and regulations. It remains to be seen whether the 2021 Bill will be enacted in its current form or be subject to further significant changes on the floor of the Parliament.

Our detailed analysis on the provisions of the bill including its impact on various sectors will follow.

*****

Key Contacts:

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner (Head - TMT)
arun.prabhu@cyrilshroff.com