Touchstone Partners

GREY MATTERS

INDIAN DATA PROTECTION BILL: JPC RECOMMENDATIONS

DECEMBER 2021

JPC Report finalised:

There may well finally be movement on the data protection law front in India in the next few months. The Joint Parliamentary Committee (the ***JPC***) responsible for reviewing the Personal Data Protection Bill, 2019 (the ***2019 Bill***) has finalised its report (the ***JPC Report***), and this is expected to be tabled before Parliament towards the end of December 2021. Whilst the text of the JPC Report is not yet publicly available, it is being reported that several changes to the 2019 Bill have been proposed, both by way of drafting amendments as well as more substantive amendments. This note looks at the key amendments that are being reported and will be updated once the JPC Report is available for review.

Key Recommendations:

Inclusion of Non-personal data (NPD)

The JPC Report recommends the scope of the proposed statute should not only cover personal data but non-personal data as well. The reasons for this apparently include the fact that a large amount of non-personal data derives from personal data which has been anonymised (and doubts about true anonymisation have been expressed) or converted into non-identifiable data, and it will be easier to have a single law and single regulator (the data protection authority proposed to be set up under the current statute) to deal with all types of data.

However, the JPC does not appear to have prepared the actual clauses or sections dealing with the regulation of non-personal data, and has merely proposed that separate regulations in this regard can be prepared under the proposed new statute which it calls the "Data Protection Act" (rather than the "Personal Data Act"),

It is relevant to mention that a committee (the ***Gopalakrishnan Committee***) was previously constituted by the Ministry of Electronics and Information Technology to formulate a framework to regulate non-personal data, which released an updated report in December 2020. This report suggested dealing with non-personal data under a separate legislation and with a separate regulator. It remains to be seen how many of the other recommendations made by the Gopalakrishnan Committee (which include sharing of non-personal data across businesses, and open access to

meta data) make their way into the final proposed legislation.

State use exemption and government powers

The original draft of the bill included a state use exemption (pursuant to which government agencies could be exempt from complying with the requirements of the statute) but this only applied in the interests of security of the state. However, the 2019 Bill recognised certain other grounds for the state use exemption, including the ground of "public order", and with no other conditions as to reasonableness or proportionality. This was widely criticised as giving the state unfettered powers, and inconsistent with the principles set out in the Supreme Court judgement that recognised privacy as a fundamental right.

The JPC Report apparently attempts to find a balance in this regard and incorporates a condition of "just, fair, reasonable and proportionate" processes to be adopted by the state if such an exemption is utilised.

However, these drafting changes (which are not yet available) have met with opposition within the JPC itself as being insufficient, and five members of the 30-member committee have moved dissent notes on this issue. The dissenting members want "public order" to be removed as a ground for using the exemption, and for judicial or parliamentary oversight for granting such exemptions.

It is relevant to mention that recent allegations that the government has used Pegasus spyware to "snoop" on Indian citizens are pending before the Indian Supreme Court. In forming an expert committee to investigate this, the Supreme Court has noted that the government's responses have not provided any light on the matter and said that the ground of "national security" cannot be evoked to avoid judicial review, especially when constitutional rights of citizens are at stake. Against this backdrop, the state use exemption in the proposed data law will likely come under a great deal of scrutiny and may well invite legal challenge.

Under the 2019 Bill, the government had the power to issue directions on policy to the data authority, which the authority was bound to comply with. It is reported that the JPC has proposed amendments which enable to government to issue directions to the authority on all matters and not just policy, and the authority will be required to comply with all such directions (and not just directions on policy).

Social Media Platforms

The 2019 Bill introduced a concept of "social media intermediaries", which would offer voluntary user verification, if they were of a substantial size. The JPC Report apparently refers to such intermediaries as "social media platforms" (***SMPs***) and has suggested some significant requirements and obligations in this regard:

- The JPC apparently notes that SMPs often have the ability to control their content and SMPs which do not act purely as intermediaries should be treated as publishers and held accountable for the content hosted.

- SMPs can also be held responsible for content from unverified user accounts

and will be mandatorily required to verify accounts. They could otherwise lose safe harbour protections.

- No SMPs will be allowed to operate in India unless the parent company sets up an office in India.

- The JPC has suggested the setting up of a statutory media regulatory authority to regulate content published, whether online, print or otherwise.

These recommendations of course have significant ramifications for social media companies, and especially international platforms. Reports suggest that such companies may well mount legal challenges if these recommendations become part of the new law. Regulation of online social media is clearly an important concern for the JPC, but questions are being raised as to whether the proposed data protection law is the correct place to address this, and also how the proposed recommendations will fit in with the recent (and controversial) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (please see our article on these rules here).

Data Localisation

Data localisation has been a key concern for the JPC.

Data localisation requirements were already set out in detail in the 2019 Bill, but the JPC Report apparently adds a requirement that a mirror copy of sensitive personal data and critical personal data which is already in possession of the foreign entities will need to be brought to India in a time bound manner. This will be an important compliance obligation for companies that currently store India-related data on servers overseas to be aware of.

The JPC has also recommended that the government must prepare an extensive data localisation policy, in consultation along with other sectoral regulators such as the Reserve Bank of India.

Data Breaches

Data security has also been a key requirement for the JPC. The JPC Report recommendations in this regard apparently include the following:

- Data breaches in relation to both personal data and non-personal data are required to be reported by notice to the data authority.

- Data fiduciaries must report all data breaches, and not just data breaches that are 'likely' to cause harm to data principals.

- Data breaches must now be reported within a prescribed time frame of 72 hours.

- It appears that data fiduciaries will be mandatorily required to report data breaches to the affected data principals.

Other Recommendations

Reports suggest that the JPC contains the following other recommendations:

- The new law should be implemented in a phased manner over a period of 24 months of the law being notified. A

period for staggered implementation was notable by its absence in the 2019 Bill, which had caused concern that many data fiduciaries would be caught unaware if the law took effect immediately.

- Data fiduciaries dealing exclusively with children's data are required to be registered with the data authority and would qualify as "significant data fiduciaries" (a type of data fiduciary that is subject to higher compliance requirements). This will be especially relevant for ed-tech companies and other companies that access and process data of minors.

- Significant data fiduciaries will need to appoint a data protection officer based in India, who will need to be part of senior management and have adequate technical knowledge.

- The right of data portability and the right to be forgotten have apparently been strengthened. Reports state that the JPC felt that portability requests should not be denied on the grounds that this could lead to trade secrets being disclosed.

- Surveillance concerns mean that data collection by hardware manufacturers and hardware equipment should also be regulated. There should be a framework that provides for monitoring, testing and certification to ensure integrity of hardware equipment and prevents any interdiction or seeding that could result in a breach of personal data.

- In light of privacy concerns regarding existing financial networks such as the SWIFT network, and the particular importance of data security in the financial sector, an alternative indigenous financial system should be developed.

- There are suggestions that the quantum of penalties (which were in line with GDPR and worked off a percentage of worldwide revenue) have been reduced but further information in this regard is not currently available.

Next Steps:

It is expected that the JPC will submit its report to Parliament in the coming weeks. However, the draft bill is not listed on the legislative agenda for the current session of Parliament and may only be taken up in the Budget session early next year.

We are of course continuing to monitor developments and will provide updates as and when further information becomes available.

Anuj Bhatia
Partner
anuj.bhatia@touchstonepartners.com

Raveena Thakkar
Associate
raveena.thakkar@touchstonepartners.com

Aastha Saily
Associate
aastha.saily@touchstonepartners.com