New data bill gives sweeping powers to govt

| | Published 13.12.19, 07:11 PM

The new Personal Data Protection Bill- 2019 represents a positive step towards finally realising a data protection and privacy law for all Indians. It introduces principles of collection limitation, data retention and purpose limitation, and strengthens the existing notice and consent framework. However, at the same time, the bill extensively broadens the exemptions granted to the government from these and other data protection obligations, giving rise to significant concerns for citizens' privacy. Let's focus on three such exemptions in this piece — Sections 35, 36 and 12.

First, let's look at Section 35 which gives the government wide powers to exempt itself from the protections guaranteed to citizens under the bill. For instance, this section empowers the central government to exempt "any" government agency from "all or any" provisions of the act with regard to processing of specified personal data. The government can also take such a step if it is satisfied that it is "necessary or expedient" to do so in the interest of sovereignty and integrity of India, the security of the state, friendly relations with foreign states and public order. In addition, the government can also be given an exemption on grounds of preventing incitement to commit any cognisable offence relating to the sovereignty and integrity of India, the security of the state, friendly relations with foreign states and public order. Section 35 marks a stark contrast from the previous version of the Personal Data Protection Bill- 2018 released by the Justice Srikrishna Committee, which only exempted the processing of data "in the interests of the security of the state".

The 2018 bill granted the exemption for the processing of personal data if the processing complied with four conditions – first, it was authorised pursuant to a law; second, it was in accordance with the procedure established by such law, made by Parliament; third, it was necessary for achieving such interests; and fourth, it was proportionate in its application. These requirements were introduced to comply with the Supreme Court judgment in the landmark Justice K.S. Puttaswamy versus Union of India (Right to Privacy) case. That unanimous ruling held that Indians have a constitutionally protected fundamental right to privacy. The judgment further held that any exemption from the application of the act should be narrowly tailored. Even then, the 2018 bill was criticised for being a near carte blanche given to the government.

However, the 2019 bill removes these safeguards entirely and replaces them with a mere requirement that the central government pass an order, recording its reasons in writing, subject to "such procedures, safeguards, and oversight mechanism to be followed by the agency, as may be prescribed." In this manner, the government has left the important task of oversight and accountability to regulations that will be notified by the Data Protection Authority directly — and hence, will not be debated in Parliament — and will likely not include judicial oversight.

Another departure from the 2018 bill lies in the Union's power to exclude the application of the entire 2019 bill. In the previous iteration of the legislation in 2018, the Justice Srikrishna Committee had imposed minimal safeguards in the exercise of the exemption by the State by first, imposing a duty on it to process the data in a "fair and reasonable", privacy-respecting manner. Second, the 2018 bill required security safeguards to be followed, including using methods such as de-identification and encryption, taking necessary steps to the protect the integrity of the personal data, and taking necessary steps to prevent its misuse. Third, the 2018 bill did not exclude the provisions of the bill that related to civil and criminal offences and penalties or the provisions pertaining to the Data Protection Authority. Unfortunately, the 2019 Bill does not even impose these minimal safeguards on the state.

The 2019 bill, thus, vests enormous power with the central government. Section 35 can completely exclude the application of the 2019 bill, and in the process, infringe on the privacy of an individual, based on its own satisfaction of the fulfilment of certain pre-conditions. In view of this, the lack of any prescribed safeguards; the lack of independent (parliamentary/judicial) oversight mechanism; as well as the removal of the requirements of legality, necessity, and proportionality are deeply troubling and likely to be struck down as unconstitutional.

Now, let's turn to Section 36. This section also exempts certain provisions of the 2019 bill for, *inter alia*, the processing of personal data in the interests of "prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force". It also departs from the corresponding provision in the 2018 bill by removing the requirements of legality, necessity, and proportionality.

Apart from this, Section 12 permits the processing of personal data without the consent of the data principal if such processing is necessary "for the performance of any function of the State authorised by law" for the provision of any service or benefit to the data principal from the state. This is a broadly worded exemption and seems to cover the use of the PDS (Public Distribution System) through Aadhaar. The requirement in the 2018 bill that sensitive personal data may be processed for the exercise of any function of the state only when it is "strictly necessary" has also surprisingly been done away with. Section 19(2) further restricts the right to data portability if the processing is necessary for "functions of the State".

The underlying theme of this new data protection bill is to give even greater power to government. This manifests itself in various other provisions such as Section 91 permitting the central government from framing any policy for the "digital economy", insofar as such policy does not govern personal data.

The granting of increased power to the government, particularly the central government, must be accompanied by increased scrutiny. Now that the bill has been referred to the joint parliamentary committee instead of the parliamentary

standing committee on information technology, it is all the more important that the bill is properly debated and various stakeholders consulted. Only then can the true promise of privacy in the Puttaswamy case be retained and flourish.

The author is an advocate practicing in Delhi