Source : www.thehindu.com Date : 2022-08-07

EXPLAINED

Relevant for: Indian Polity | Topic: Parliament - structure, functioning, conduct of business, powers & privileges and issues arising out of these

The Bill that was tabled in the Lok Sabha on December 11, 2019, had undergone intense scrutiny by a Joint Parliamentary Committee.

The story so far: On Wednesday, August 3, the Centre government withdrew the Personal Data Protection Bill that it had tabled in the Lok Sabha on December 11, 2019. The Bill, which had undergone intense scrutiny by a Joint Parliamentary Committee (JPC), would now be replaced by "a new bill that fits into the comprehensive legal framework," as per the government's statement on the withdrawal. Information Technology Minister Ashwini Vaishnaw has said that the new Bill is in advanced stages of preparation and may be tabled in the Budget session next year.

Editorial: A fresh opportunity

In the seminal *Justice K.S. Puttaswamy (Retd) vs Union Of India case*, the Supreme Court of India ordered in 2017 that the right to privacy is an intrinsic part of the right to life and personal freedom guaranteed by the Indian constitution. In the light of this judgment, and the abounding concerns around how large tech platforms were handling the personal data of its Indian users, the Centre in 2017 set up an expert committee chaired by retire Supreme Court Justice B.N. Srikrishna to formulate a regulatory framework for data protection. The Srikrishna committee submitted its report and a draft for the Data Protection Bill to the Ministry of Electronics and Information Technology on July 27, 2018.

The Bill that was tabled by the Ministry in Parliament over a year later was, however, criticised by Justice Srikrishna for giving much more control to the Central government over the data than envisaged in the committee's draft.

The JPC that then deliberated on the Bill submitted its report in November, 2021, clearing clause 35, the provision that enables government agencies to circumvent provisions of the law citing "public order", "sovereignty", "friendly relations with foreign states" and "security of the state". The opposition members of the JPC had submitted strong dissent notes along with the report.

Despite the government retaining its access to data, it has withdrawn the Bill now citing the significant number of amendments, recommendations, and corrections suggested by the JPC. The JPC's 542-page report has 93 recommendations, 81 amendments and suggested 97 corrections and improvements to the Bill. One of the key recommendations is widening the ambit of the Bill to cover all data instead of just personal data — thus moving it considerably away from its *Puttaswamy* origins. The stated view of the government is that in the face of such a radical overhaul, it is better to bring in a new Bill.

Alongside this, the government has also said that it received several concerns from the tech industry — specifically from Indian start-ups — regarding the stipulations on data localisation in the Bill.

Personal data was defined in the Bill as "any characteristic, trait, attribute or any other feature information" that can be used to identify a person. The Bill also identified a sub-category of Sensitive Personal Data, such as details on a person's finance, health, sexual orientation and practices, caste, political and religious beliefs, and biometric and genetic data. It also created

Critical Personal Data category, which was “personal data as may be notified by the Central Government” in the future.

The Bill stated that while Sensitive Personal Data can be transferred abroad for processing, a copy of it must be kept in India. Critical Personal Data can be stored and processed only in India. It also stipulates the conditions under which sensitive data can be sent abroad, such as government authorised contracts.

Several countries have such localisation provisions, considering the strategic and commercial implications of data, the “new oil”. However, businesses both big and small, international, and domestic, have issues with such localisation.

Indian start-ups have raised the issue that the infrastructure needed to comply with the localisation stipulations will be a huge drain on their resources. Start-ups also often depend on international companies for services such as customer management, analytics and marketing, which will require them to send data on their customers abroad. Data localisation requirement would not only reduce their choices on such services but also burden them with compliance processes.

The compliance requirements have implications for the larger U.S.-based tech companies as well, with reports indicating that umbrella organisations of U.S. businesses were lobbying against the Bill.

One of the JPC recommendations would also have been of particular concern for social media companies as it sought to move them from the category of online intermediaries to content publishers, thus making them responsible for the posts they host.

Our code of editorial values

END