Source : www.thehindu.com Date : 2022-08-22

WHAT NEXT ON DATA PROTECTION?

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

The withdrawal of the Personal Data Protection Bill from Parliament came as a surprise, particularly after so much effort was put into it over the last five years. Between August 2017 and July 2018, a 10-member committee chaired by a former Supreme Court judge drafted the Bill. The committee included four senior government officials. The Bill was then revised by the government, approved by the Cabinet, and tabled in Parliament in December 2019. Subsequently, a joint parliamentary committee, or JPC, comprising a majority of BJP members, reviewed the bill and submitted its report in December 2021. The withdrawal does not reflect well on the government, the entire process having been played out under its regime. This also increases uncertainty about the future of privacy regulation in India.

One way to understand this decision is to go back to the genesis of this law, which arose out of the *JusticeK.S. Puttaswamy v. Union of India* case where the court held that the right to privacy had both a positive and negative aspect. The former implies the need for the state to actively take measures to protect an individual's privacy. Thus, the government was more or less forced to initiate the drafting of a data protection law. This experience also tells us something about the limits of judicial inducement for regulation, for which active effort of the other two branches of the state is needed. The options of delay and dilution are always available.

The growing importance of the digital economy and the broad scope of the proposed law also contributed to contestations between stakeholders as the law was being deliberated. Shaped by different interests and incentives, the state, industry, and advocacy groups all have very different expectations of what a data protection law should look like. For instance, for domestic industry such a law represents a compliance hurdle which could put it at a disadvantage. However, a law can also promote regulatory certainty, thereby opening up the possibility of increased data flows and the growth of data processing business. For the state, a law could limit intrusive data processing by state agencies, but it could also promote geopolitical, strategic or regulatory interests. Similarly, individuals could benefit by the restrictions on harmful data processing, but on the other hand, a poorly drafted law could legitimise certain intrusive practices.

Each version of the law — the 2018 Bill of the Srikrishna Committee, the 2019 Bill introduced in Parliament, and the version of the JPC in 2021 — faced different types of critique from different stakeholders. For instance, law enforcement interests were seen as being obstructed by the 2018 draft, leading to broad exemptions being provided in the 2019 Bill.

However, what appears striking is the consistent dilution of the focus on data privacy from the 2018 version onwards. From being the centerpiece of the legislation, privacy protection was increasingly being seen as one of several objectives being pursued. This was seen most clearly in the JPC's recommendations, which sought to significantly revise the scope of the law. The JPC recommended moving away from a personal data protection law towards a law to govern the entire data ecosystem. It further suggested putting in place a number of broader restrictions on social media and other entities. This attempt to solve multiple problems in the digital ecosystem saw an already broad law being turned into an omnibus Bill. This made one question the ability to properly implement it. In addition, the provisions relating to many issues were lacking in detail. For example, the provisions related to processing of data by the state, governance of non-personal data and the regulation of social media could all have been fleshed out with greater substantive and procedural detail, which is required to balance the complex competing interests at hand.

Looking forward, there are two critical issues – the form that a new law will take, and the nature of protections it will offer.

On the first issue, the government has suggested that it will introduce multiple legislation comprising a new comprehensive legal framework. This is the right approach, as trying to fit all objectives related to the digital ecosystem or even data governance into one Bill would be a mistake. It is healthy to maintain some polycentricity in the governance of a complex digital economy, and different laws and agencies should co-exist. It would be ideal if each bill addressed a single coherent set of objectives: For instance, one personal data protection bill should not be burdened with other objectives. Similarly, separate laws could deal with issues concerning state surveillance, or issues in the data economy such as dealing with competition-related concerns arising out of the monopolisation of data by certain entities. Over time, such a system may lead to more balanced and beneficial results. In the short term, however, the government would do well to put in place a specific personal data protection law – given the effort already dedicated to this (and the significant areas of agreement amongst stakeholders).

Editorial | A fresh opportunity: On the rollback of the Personal Data Protection Bill

The second issue is the nature of privacy protection any new law will provide to individuals. The 2018 law, on which future drafts were based, borrowed heavily from the rights-based European General Data Protection Regulation. This framework was however criticised by some due to its perceived unviability in the Indian context. For instance, creating a cross-sectoral data protection entity with the power to take significant coercive action is seen as problematic given the rule of law, capacity and regulatory constraints in India. Some of these issues could be addressed in creating a new data privacy law.

Also read | Consider global learnings for new data protection law, Nasscom urges government

First, it should build in a risk-based approach to data protection, so that the regulatory focus is directed towards addressing sources of potential harm. Second, based on risk assessments, the law could enable co-regulation and self-regulation (with the regulator acting as a backstop). These could reduce compliance burdens on entities without significantly affecting rights protection. Third, the current version of the law was weak on accountability measures for the data protection regulator. The new Bill should include more provisions to ensure that the regulator uses its powers well. These include provisions relating to appointments, consultations, reporting, and so on. Fourth, even while the law is being drafted, the government should invest in building some administrative capacity to implement it, so that when the law is eventually passed, implementation can begin soon after. This has been previously done with SEBI and PFRDA. Finally, it is vital that any new law is framed based on transparent and meaningful consultations with all stakeholders.

Rishab Bailey is an advocate and technology policy researcher, associated with the xKDR Forum, Mumbai; and Suyash Rai is a Deputy Director and Fellow at Carnegie India

Our code of editorial values

END