Source : www.thehindu.com Date : 2023-07-21

INDIA'S DATA PROTECTION LAW NEEDS REFINEMENT

Relevant for: Indian Polity | Topic: Indian Constitution - Features & Significant Provisions related to Fundamental Rights, Directive Principles and Fundamental Duties

July 21, 2023 12:08 am | Updated 01:36 am IST

'India must guard against the risks of enacting a law that is toothless in effect' | Photo Credit: Getty Images

India is no Europe, and this seems especially true in the face of a task such as drafting and conceptualising a data protection law for over 1.4 billion Indians. The European Union's (EU) data protection law, i.e., the General Data Protection Regulation (GDPR), came into force in the middle of 2018 and achieved widespread popularity as arguably the most comprehensive data privacy law in the world. However, the GDPR has been saddled with challenges of implementation and risks being relegated to the status of a paper tiger. Although the EU's challenges may be due to its unique legal structure, India must guard against the risks of enacting a law that is toothless in effect.

This deliberation becomes increasingly relevant as the Indian government is likely to table India's fresh data protection law in the ongoing monsoon session of Parliament (July 20-August 11). Late last year, the government released the Digital Personal Data Protection (DPDP) Bill, 2022 for public consultation. This is its third recent attempt at drafting a data protection law. While the draft released for public comments was not as comprehensive as its previous versions, news reports suggest that the government may present a Bill that is largely similar. Considering this, critical gaps remain in the DPDP Bill that would affect its implementation and overall success.

In its scope and definition, the DPDP Bill only protects personal data, that is any data that has the potential to directly or indirectly identify an individual. In the modern data economy, entities use various types of data, including both personal and non-personal data to target, profile, predict, and monitor users (non-personal data is typically anonymous data that does not relate to a particular individual — for example, aggregate data on products which numerous users look at between 9 p.m. and 11 p.m. on Amazon). Often, this non-personal data when combined with other datasets can help identify individuals, and in this way become personal data, impacting user privacy.

For instance, anonymous datasets about individual Uber rides in New Delhi can be combined with prayer timings to identify members who belong to a certain community, which could include their home addresses. This process of re-identification of non-personal data poses significant risks to privacy. Such risks were accounted for in previous versions of India's draft data protection Bill, in 2018 and 2019, but do not find a place in the latest draft. By not recognising

these risks, the DPDP Bill is very limited in its scope and effect in providing meaningful privacy to Indians. A simple and effective solution — as in the earlier versions — would be to add a penal provision in the Bill that provides for financial penalties on data-processing entities for the re-identification of non-personal data into personal data.

Another gap is the inability of the proposed data protection board to initiate a proceeding of its own accord. Under the Bill, the board is the authority that is entrusted with enforcing the law. The board can only institute a proceeding for adjudication if someone affected makes a complaint to it, or the government or a court directs it to do so. The only exception to this rule is when the board can take action on its own to enforce certain duties listed by the Bill for users. This is for the adjudication of disputes between the law and users — for example, an obligation on users not to register a false or frivolous complaint with the board, and not between users and data-processing entities.

In the data economy, users have diminished control and limited knowledge of data transfers and exchanges. Due to the ever-evolving and complex nature of data processing, users will always be a step behind entities which make use of their data. For example, a food delivery app can take all my data and sell it to data brokers in violation of my contractual relationship with them. Individually, I may have little resources or incentive to approach the data protection board.

The board, on the other hand, may be in a better position to proceed against the food delivery app on its own — on behalf of all such affected users.

This is not a novel suggestion. The Competition Commission of India, which is responsible for the enforcement of India's antitrust law, has the power to initiate inquiries on its own (and utilises it frequently). Again, a simple way to do this would be to have a provision in the DPDP Bill that allows the data protection board to initiate complaints on its own.

These are not the only gaps in the DPDP Bill, but finding solutions to them would help address challenges in implementation in a significant way and make for a more future-proof legislation.

Shashank Mohan is Programme Manager at the Centre for Communication Governance, National Law University Delhi