AADHAAR

TIMES OF INDIA, Delhi, 30.7.2018

Page No. 12, Size:(19.83)cms X (17.95)cms.

A Free & Fair Digital Economy

Draft data protection bill asserts our sovereignty and safeguards citizens' interests

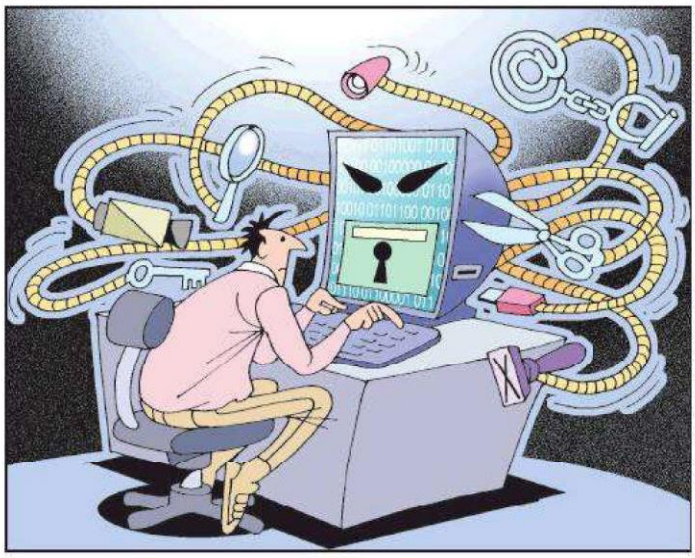
Arghya Sengupta

The draft data protection law recommended by the committee of experts to the government of India is a template of how the Global South can safeguard the interest of its citizens and assert its sovereignty in a digital age dominated by giant American tech corporations. It recognises the immense power of data to empower citizens by providing a range of services accessibly and affordably. It is equally cognisant of the debilitating harms that unexpected sharing of data might cause to individuals, tracking their online behaviour, storing their preferences, often on intimate matters, and breaching their privacy.

To understand the importance of the proposed law, one needs to step back from technical details of legal drafting and understand the larger headwinds in the global digital economy. The growth of the internet has been the single most revolutionary innovation of our time. Like most good innovations, it too has changed over time. In the last decade, the internet has seen a distinct shift away from a true commons to a cluster of fenced spaces.

Take a simple example – imagine if one could only send emails from Outlook accounts to Outlook accounts alone or Gmail accounts to Gmail accounts alone. The thought is patently absurd. Yet this is precisely what happens when playlists on Saavn cannot migrate to Gaana, or messages from WhatsApp cannot be delivered to Snapchat. This change of business model – from service delivery to targeted advertising – is owing to the recognition of the immense potential to monetise personal data. Exclusionary control over personal data is critical to this business model.

If the foundation of the digital economy is to be personal data and the quest to gather it the new Gold Rush for corporations, the autonomy and privacy of the Indian citizen must be fully secured. This is the constitutional mandate of the Puttaswamy judgment that has been translated into actionable law by the committee in four primary ways.



First, the individual, denoted worldwide as the data 'subject' is, in the committee's formulation – the data 'principal'. The entity who seeks her data, instead of being termed the data 'controller' is the data 'fiduciary'. This is not a mere symbolic change.

When an individual gives her personal data to a railway ticket booking website, she expects it to be used only to book her railway ticket and not to be controlled by the website, irrespective of what the legalese-filled consent form might contain. This is because the relationship between the individual and the website is one of trust – the individual expects her data to be used in a certain way and trusts that the entity will do so. This is the cornerstone of a fiduciary relationship. The bill, by making all data processing entities, fiduciaries, holds them liable if such trust is betrayed.

Second, the consent framework is itself fundamentally modified. Today, each one of us is perhaps culpable of saying "I agree" to long consent forms on our smartphones while downloading apps without really knowing what we agree to. As a result, an app that provides me with a taxi can read my messages, and an app to book tickets can access my photos.

Entities will only be allowed to collect information necessary for their service and the purposes to which such information will be used will be clearly communicated. Taxi apps cannot read my messages

The bill addresses this anomaly by introducing the principles of collection and purpose limitation. Entities will only be allowed to collect information necessary for their service and the purposes to which such information will be used will be clearly communicated. Taxi apps cannot ordinarily, in this formulation, read my messages.

Third, if any individual is aggrieved today that their data is being used in a manner that breaches their privacy, there is no easily accessible remedy. The bill sets up a Data Protection Authority (DPA), an independent body with an adjudication wing and offices across the country. The DPA has the power both to penalise companies up to 4% of their worldwide turnover and compensate individuals for harm suffered. Critically, if the data fiduciary is a government department or a public sector entity, it too will be liable to pay a penalty up to Rs 15 crore.

Finally, India has the unfortunate distinction of being a country that is long on prescription and short on enforcement. To prevent this law from going the same way, the committee recommends a strict mandate for local storage of data. Some critics view local storage as a fig leaf for surveillance. This is ill-conceived fear mongering. Local storage of data does not mean a giant honeypot allowing the state to play big brother.

It envisages hundreds of data centres in the country on the strength of which India can build an Artificial Intelligence ecosystem, create jobs and remain at the vanguard of innovation in the world. It equally allows the state to hold private entities accountable if personal data that they hold is needed for security of the state and prevention of crime. As the Supreme Court itself has noted, these are critical functions of the state.

This state was created in 1950, when our founding fathers wrote a Constitution that enshrined freedom and fairness as the cornerstone of our new Republic, ending our dominion status. In 2018, the bill and report channel the same spirit and show the way for India to become a digital leader and not remain a mere digital dominion. While debate on the provisions of the bill, will and should continue, we must all work together to give India and the Global South, the free and fair digital economy that we deserve.

The writer is Research Director, Vidhi Centre for Legal Policy and a member of the Committee of Experts which drafted the Personal Data Protection Bill, 2018. Views are personal