Source : www.thehindu.com Date : 2019-12-27

THE DATA PROTECTION BILL ONLY WEAKENS USER RIGHTS

Relevant for: Developmental Issues | Topic: E-governance - applications, models, successes, limitations, and potential incl. Aadhaar & Digital power

In the continuing social churn and widespread citizen protests, it would seem out of place to direct thought towards issues such as data protection. The Personal Data Protection Bill, 2019, **which was introduced in the Lok Sabha this month**, is a revolutionary piece of legislation that promises to return power and control to people in our digital society. Pending deliberation before a Joint Parliamentary Committee, it is intimately connected to the very same fundamental rights and constitutional principles that are being defended today on the streets and in the fields.

The Bill has seen serpentine movement, passing expert committees, central ministries and then the Lok Sabha in the winter session. Before focusing on the nuances and finer details which merit deliberation we must take a step back to look at the broader politics of personal data protection. This would help contextualise the legislative proposal and understand the degree of protection which is limited by overboard exceptions in favour of security and revenue interests.

The rise of the national security narrative has not been gone unnoticed by seasoned political observers. What is novel is its intersection with technology. This is central to several policy and political pronouncements by the present government. In many ways, it is a continuation of the politics of securitisation of the government from its previous term. For instance, the Bharatiya Janata Party's manifesto (sankalp patra) released before the general election 2019 provides useful insight where it states appropriate technological interventions centred around Aadhaar. This shrugs off any recognition of its contested legality before the Supreme Court which ruled on the fundamental right to privacy. Privacy is mentioned just once in this voluminous document — 49 mentions of 'security' and 56 mentions of 'technology'.

This is a trend which continues. The President of India's address to Joint Sitting of Parliament on June 20, 2019 — fresh from the results of the general election — proclaimed that "my government is committed to that very idea of nation-building, the foundation for which was laid in 2014". The priorities of the government are clearly charted out with zero mention of privacy or data protection; there are 18 mentions of 'security' and eight of 'technology'. This familiar template is again found in the Prime Minister's Independence day speech on August 15, 2019 which focussed on dramatic social change. He noted: "I believe that there should be change in the system, but at the same time there should be a change in the social fabric." There is zero mention of 'privacy' or 'data protection'; however there are seven mentions of 'security', six on 'technology' and five for 'digital'. There may be government policy documents that may emphasise or contradict these assertions. However these statements made by high public officials at historic times when they may be widely viewed by large number of Indians are deserving of primacy. They reveal, at the very least, a pecking order in terms of viewing both technology and security as high priorities in governance objectives.

As Edward Snowden explains in his *Permanent Record*, there is a symbiotic relationship between the financial model of large online platforms and security interest. They both feed off personal data and the attention economy, where platforms gather this data and the government then seeks access to it. In India this is being taken a step further. The government is seeking to not only access data but also collect it and then exploit it — making it an active data trader for the generation of revenue to meet its fiscal goals.

First, the scale of data collection is ambitious and broadly contained in the ‘Digital India’ programme; on its website it says: “to transform the entire ecosystem of public services through the use of information technology…”. Here, all elements of a citizen-state interaction are being data-fied. In the view of some technologists, this also fulfils geostrategic goals when personal data is viewed as strategic state resource. However, this poses grave risks to the right to privacy. These become evident from a casual reading of the national Economic Survey of 2019, which in Chapter 4 devotes an entire chapter on the fiscal approach towards personal data. In a “Chapter at a glance” it says: “In thinking about data as a public good, care must also be taken to not impose the elite’s preference of privacy on the poor, who care for a better quality of living the most.”

Second-order effects of the Personal Data Protection Bill

Two tangible examples show the operation of this policy framework. The first is with respect to the recent sale of vehicular registration data and driving licences by the Ministry of Road Transport and Highways. Here, quite often, the principles of a data protection law would conflict with these uses as it would break the fundamental premise of purpose limitation. This principle broadly holds that personal data which is gathered for a specific purpose cannot be put to any other distinct use without consent of the person from whom it was acquired. The second is an expert committee (headed by Kris Gopalakrishnan, Chairperson, Infosys) on what is termed “community data”. While the definition of such, “community data” is contested, as per the note it is plainly obvious this is again to serve fiscal interests of the state and technology businesses when it states that such data “is critical for economic advantage”.

The existing draft of the Data Protection Bill is reflective of a political economy that is motivated towards ensuring minimal levels of protection for personal data. It has a muddled formulation in terms of its aims and objectives, contains broad exemptions in favour of security and fiscal interests, including elements of data nationalism by requiring the compulsory storage of personal data on servers located within India.

From its very preamble it seeks to place the privacy interests of individuals on the same footing as those of businesses and the state. Here, by placing competing interests on the same plane, two natural consequences visit the drafting choices within it. First, the principle of data protection to actualise the fundamental right to privacy is not fulfilled as a primary goal but is conditioned from the very outset. Second, by placing competing goals — which contradict each other — any balancing is clumsy, since no primary objectives are set. This results in a muddy articulation that would ultimately ensure a weak data protection law.

This present draft of the Bill comes as a disappointment especially after the emphatic judgment by the nine-judge Bench of the Supreme Court on the Right to Privacy. The judgment contains categorical language that the Bill is a measure to actualise the fundamental right. However, this draft serves a political economy which at first blush appears attractive in its promise of taking us away from the dull maxims of constitutionalism and delivering us a digital utopia. Again, this was best phrased by the Prime Minister when he stated at the Digital India dinner on September 26, 2015, at San Jose, California: “... technology is advancing citizen empowerment and democracy that once drew their strength from Constitutions.”

Hence, on a broader read, the Data Protection Bill is not a leaky oil barrel with large exceptions, but it is a perfect one. It will refine, store and then trade the personal information of Indians without their control; open for sale or open for appropriation to the interests of securitisation or revenue maximisation, with minimal levels of protection. For this to change, we have to not only focus on red-lining the finer text of this draft but also reframing large parts of its intents and objectives.

Apar Gupta, Executive Director of the Internet Freedom Foundation, is a Delhi-based lawyer