Power over privacy: New Personal Data Protection Bill fails to really protect the citizen's right to privacy

Earlier this year, in April, a data breach in the Election Commission of Philippines led to the leakage of personal information of over 55 million eligible voters on a searchable website: including names, addresses and date of birth. This was not the first data breach from the Election Commission. After the first, which took place in March 2016, where 340 GB of voter data was published online by a group of hackers called LulzSec Pilipinas, the National Privacy Commission of Philippines found that the Election Commission had violated the Data Privacy Act of 2012, and recommended criminal prosecution of its chairman, finding him liable when the agency failed to dispense its duty as a "personal information controller".

It's 2019, and that recommendation has still not been acted upon, because the National Privacy Commission of Philippines only has recommendatory powers for criminal prosecution. Meanwhile, data breaches continue at the Election Commission of Philippines.

Between 2017 and 2018, Aadhaar related personally identifiable data of several Indian citizens, including names, addresses, bank account numbers, in some cases pregnancy information and even religion and caste information of individuals, was published online by Indian government departments. The Centre for Internet and Society, in a report, estimated that personally identifiable data for 130-135 million Indian citizens had been leaked, thus putting them at risk. 210 government websites had made Aadhaar related data public, UIDAI confirmed in response to an RTI in 2017.

No one was held liable. There was no data protection law, no data protection authority, no criminal prosecution was recommended. Around that time, the Indian government was instead arguing in the Supreme Court that privacy isn't a fundamental right under the Indian Constitution. Illustration: Ajit Ninan

What we can learn from these two instances is that for the enforcement of a citizen's right to privacy, and ensuring that no one takes the protection of data lightly, there needs to be a strong privacy law that holds even the government responsible, and above all, a strong data protection authority that is independent and has powers to penalise even government officials. On some of these counts, the Personal Data Protection Bill, 2019, disappoints.

First, members of the Data Protection Authority will no longer be appointed by independent entities from diverse backgrounds: where they were previously going to be appointed by a committee comprising the Chief Justice of India or a Supreme Court judge, the Cabinet secretary, and an independent expert, the power to appoint members to DPA now rests solely with government officials, including the appointment of adjudicating officers. In addition, the central

government, in the interest of "national security, sovereignty, international relations and public order, can issue directions to DPA, which DPA will be bound by. Powers of DPA have also been reduced: while in the previous version of the bill, DPA had the sole power to categorise data as sensitive personal data, in the current version, the power rests with the central government, albeit in consultation with DPA. The central government will also notify any social media company as a significant data fiduciary, and not DPA. Only the central government can determine what critical personal data is, and not DPA.

This dependence on the government for appointments, functions and definitions, will invariably impact the independence of DPA, and even though the 2019 version of the bill gives it the authority to fine the state a maximum of Rs 5-15 crore, depending on the offence, i'd be surprised if this ever happens.

The bill does create significant exceptions for the state to acquire and process data, and an opportunity to create a base for surveillance reform in the country has been lost. The previous version of the bill had brought some sense of safety against mass surveillance, when it included the condition that processing of data by the government must be "necessary and proportionate", drawing from Supreme Court's historic right to privacy judgment. This is particularly important given that the bill also gives power to the government to exempt any agency from the provisions of the bill for processing of personal data, which includes acquiring data from any public or private entity.

Effectively, this means that government agencies may be exempt from any scrutiny by DPA, and can even collect data from third parties (for example, fin-tech companies, health-tech startups) without the user even knowing. Forget recommending criminal prosecution for mass surveillance, India's DPA won't even be able to fine a government agency for such a violation of the fundamental right to privacy. The government also has vast exceptions for data processing: "for the performance of any function of the state authorised by law".

This aside, one of the more curious clauses in the bill is around non-personal data. The government, a few months ago, constituted a committee led by Infosys co-founder Kris Gopalakrishnan to look into the governance of non-personal data. Non-personal data, as the term suggests, is any data that is not related to an individual. In the bill, the government has given itself the right to acquire this data, which is essentially a company's intellectual property, to "promote framing of policies for digital economy". Why non-personal data finds a mention in a Personal Data Protection Bill is beyond comprehension, and this move will not inspire much confidence in businesses operating in India, when the state claims eminent domain over intellectual property.

It's unfortunate minister Ravi Shankar Prasad is sending the bill to a select committee, given the fact that such significant changes to the bill should have led to another public consultation.

December 11, 2019 Nikhil Pahwa in TOI