Source : www.thehindu.com Date : 2022-11-23

A DATA PROTECTION BILL THAT PROTECTS STATE SURVEILLANCE

Relevant for: Science & Technology | Topic: IT, Internet and Communications

Qatar World Cup 2022France 2-1 Australia LIVE: Giroud gives the lead after Rabiot’s leveler

November 23, 2022 12:15 am | Updated 02:07 am IST

The Ministry of Electronics and Information Technology released the Digital Personal Data Protection Bill, 2022, on November 18. The journey towards a data protection legislation began in 2011 when the Department of Personnel and Training initiated discussions on the Right to Privacy Bill, 2011. As per an Office Memorandum dated September 29, 2011, the then Attorney General, Goolam Vahanvati, opined that conditions under which the government can carry out “interception of communication” should be spelt out in the Bill. This opinion was also echoed by the Group of Experts on Privacy, headed by Justice A.P. Shah, in 2012. The report of the group emphasised the need to examine the impact of the increased collection of citizen information by the government on the right to privacy. Since then, civil society organisations, lawyers and politicians have consistently demanded surveillance reform, highlighting how personal data can only be protected when the government’s power to conduct surveillance of citizens is meaningfully regulated. However, like its predecessors, the latest Bill also fails to confront India’s growth into a surveillance society.

The surveillance architecture in India comprises mainly of Section 5(2) of the Indian Telegraph Act, 1885; Section 69 of the Information Technology Act, 2000; and the procedural rules promulgated under them. But this architecture does not meaningfully define the grounds under which, or the manner in which, surveillance may be conducted. It also does not contain safeguards such as ex-ante or ex-post facto independent review of interception directions. The concentration of power with the executive thus creates a lack of accountability and enables abuse. Evidence for this emerges not only from instances of political surveillance, but also from the slivers of transparency that accidentally emerge from telecom companies. For instance, submissions by Airtel to the Telecommunications Department, as part of the public consultation process for the Indian Telecommunication Bill, reveal that excessive data collection requests are already a reality. Airtel has asked the government to share the costs it incurs to comply with the increasing demands from law enforcement agencies to carry out surveillance.

Apart from outright surveillance, unfettered collection and processing of citizen data for other purposes, such as digital governance, raise concerns. Agitation over the nature of the surveillance architecture was voiced by the Supreme Court in its right to privacy decision in 2017 and by the Justice B.N. Srikrishna Committee in 2018. However, all iterations of the data protection legislation since — the draft Personal Data Protection Bill, 2019, the draft Data

Protection Bill, 2021 and the 2022 Bill — have no proposals for surveillance reform. Worse, personal data can be processed even without the person's consent.

Like previous iterations, Clause 18(2) of the 2022 Bill allows the Union government to provide blanket exemptions for selected government agencies. However, this Bill is more egregious than previous iterations as it permits exemption to private sector entities that may include individual companies or a class of them, by assessing the volume and nature of personal data under Clause 18(3). Comparative legal regimes, which, as per the explanatory note, were considered before proposing the Bill, do not contain comparable provisions. Such blanket exemptions to state agencies, let alone private corporations, are absent in foreign legislations. While the existing or proposed legislations in the European Union and in the U.S. permit security agencies to claim exemptions on a case-by-case basis, depending on why they are collecting personal data, they do not contain blanket exemption powers to an entire government entity. Further, other jurisdictions exercise meaningful oversight over state surveillance. For instance, the Investigatory Powers Tribunal in the U.K. is authorised to hear complaints against misuse of surveillance powers and can impose monetary penalties in case of a breach. Under the new Bill in India, exempted state agencies and private entities will not be within the purview of the Data Protection Board, the body responsible for imposing penalties in case fiduciaries infringe privacy.

Interestingly, the explanatory note accompanying the Bill elaborates on the seven principles it seeks to promote, including transparency, purpose limitation, data minimisation, and preventing the unauthorised collection of personal data. But when matched against the actual provisions, the Bill appears to serve a rhetorical value. This can also be noticed by the government's refusal to share statistical data on the number of surveillance orders issued yearly, thereby hampering any meaningful transparency. Further, in direct violation of purpose limitation, inter-departmental sharing of data is not only allowed, but encouraged by draft policies such as the draft National Data Governance Framework Policy, 2022, facilitating the creation of comprehensive profiles of citizens. In addition, provisions of other legislation, such as the Criminal Procedure (Identification) Act, 2022, which allows for overzealous collection and storage of biometric data for 75 years, are in direct contrast with the principles of data minimisation and prevention of unauthorised collection of personal data.

Editorial | Persisting issues: On the new data protection bill

The preamble to the 2022 Bill states that the purpose is to protect the personal data of individuals and ensure that personal data is processed only for lawful purposes. Unfortunately, by choosing to protect state surveillance, the new Bill fails to fulfil its mandate of protecting the right to privacy of citizens.

account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END