Source : www.thehindu.com Date : 2022-01-10

CONTROL RATHER THAN PRIVACY

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

Clause 12 of the Personal Data Protection Bill, 2019 provides exemptions for the government and government agencies and Clause 35 exempts government agencies from the entire Act itself. | Photo Credit: Getty Images/iStockphoto

In India, where the personal data of citizens are at the mercy of companies and government and where is no privacy law, the *Puttaswamy* judgment and the Justice B.N. Srikrishna committee report that led to the Personal Data Protection Bill of 2019 came as a ray of hope. But the Joint Committee report on the Bill has failed to provide a robust draft legislation ensuring the privacy of citizens. Instead, it has carved out an architecture for a surveillance state.

Under the Constitution, fundamental rights are enforced against the state and its instrumentalities and not against private bodies. The *Puttaswamy* judgment held that the right to privacy is a fundamental right. However, the report has divided the digital world into two domains — government and private — and is based on the presumption that the question of right to privacy emerges only where operations and activities of private entities are concerned. Clause 12 of the Bill provides exemptions for the government and government agencies and Clause 35 exempts government agencies from the entire Act itself. Clause 12, which says personal data can be processed without consent for the performance of any function of the state, is an umbrella clause that does not specify which ministries or departments will be covered. Further, the Bill says, “harm includes any observation or surveillance that is not reasonably expected by the data principal”. This means if you install any software in your computer and the software violates the principle of privacy and data get leaked, the complaint of the data principal will not be legally tenable as the defence will be that ‘once you have installed the software, you should have reasonably expected this level of surveillance’. The government can use these provisions as a means of control and surveillance.

Data Protection Bill | Nation’s interest always trumps individual’s interest, says JPC chief

If private entities can be given a transition time to comply with the Act, why should the same not be extended to government entities? Why should they be given blanket exemption instead? The Committee has failed to provide formidable firewalls to protect the privacy of individuals and has also carved out a mechanism for government control over personal data. The provisions are ultra vires of the judgment on privacy.

For compliance with the provisions of the Act, a data protection authority (DPA) has to be appointed. The Bill elaborates on the functions and duties of the DPA. It is doubtful whether a single authority will be able to discharge so many functions in an efficient manner. The terms and conditions of appointment of the DPA also raise concerns. Unlike the Justice Srikrishna committee report which provided for a judicial overlook in the appointments of the DPA, the Bill entrusts the executive with the appointments. Although the report expanded the committee, the power to appoint the panelists vests with the Central government. While ensuring the protection of citizens’ fundamental right, it is necessary that the authority entrusted with the responsibility should work independently. Clause 86 says, “Authority should be bound by the directions of the Central Government under all cases and not just on questions of policy”. This makes the DPA duty-bound to follow the orders of the government. This weakens its independence and gives the government excessive control. Further, the appointment of the authority violates the principle of federalism. There is internal data flow and the States are key stakeholders in the process.

Even if the proposed central authority issues directions to allow processing of data on the grounds of ‘public order’, it is important to note that ‘public order’ is an entry in the State List. If the pith and substance of the legislation are related to the State, then it has to be monitored by the State Data Protection Authority.

One of the objectives of the Bill is to promote the digital economy. But by including non-personal data within the ambit of the Bill, the Joint Committee has put a huge compliance burden on the economy. This will hit the MSME sector and small businesses harder as technical processes involving data-sharing are very expensive. The government-constituted panel headed by S. Gopalkrishnan also opposed the idea of including non-personal data in the Bill. Mandatory data localisation, it is estimated, will squeeze the economy by 0.7-1.7%. This may also invite similar measures by other sovereign countries which will hamper smooth cross-border flow of data.

The report has raised more questions than it has solved. In its present avatar, the Bill is more about surveillance and control than privacy. At the time of passage of the Bill, loopholes must be plugged so that India can have a robust data protection law.

Jaiveer Shergill is a Supreme Court lawyer and National Spokesperson, the Indian National Congress

Our code of editorial values

The national law universities need to look at intra-collaboration and work on becoming multi-universities

END