



Na Vijayashankar

An Orwellian State?

There are concerns that the Bill is dangerous as it will give the government access to citizens' data. But is privacy as important as protecting a nation's security?

PRIVACY has its boundaries. The Right to Privacy is fundamental but not absolute. But often, even wise men get carried away as is indicated by the copious criticism being heaped on the Personal Data Protection Bill, 2019 (PDPB-2019). "Privacy" as a concept is a "state of mind" and a "feeling of being left alone". Neither the Supreme Court nor experts have been able to define it precisely and it remains an enigma of its own. Trying to protect an enigmatic concept through regulation of the "information" that influences the "mental state" is not easy. Further, ensuring that the regulations satisfy every person who has a different "state of mind" does pose an impossible challenge.

The conflict between the "privacy" of one person and the "security" of another is eternal. A government needs to have its hands free for "intelligence gathering". This includes surveillance, without which the country and its people are unsafe. "Security" is, therefore, as much a fundamental right as "privacy" and legislation such as PDPB-2019 cannot be seen myopically as if "privacy" is an absolute right.

But rejecting the right of the government to maintain national security through regulated invasion of privacy will disturb the mental peace of millions of citizens who wouldn't know if the

person standing next to them is a terrorist. It is only faith in security screening that emboldens us to travel by air without a care that the plane could get hijacked or bombed. This feeling of "safety" is as important for most citizens as "privacy".

However, there has been quite a bit of criticism of the Bill even from Justice BN Srikrishna who headed the committee that drafted it. Parts of the Bill which exempt government agencies from some or all provisions are "dangerous" and can turn India into an "Orwellian State", he said. "They have removed the safeguards. That is most dangerous. The government can at any time access private data or government agency data on grounds of sovereignty or public order. This has dangerous implications," Justice Srikrishna reportedly said.

But it is necessary to examine the draft Bill, recognising the presence of multiple stakeholders such as

the individual, corporates, the government and law enforcement, all of whom have different perceptions of how the data protection legislation should be conceived.

In the past, there have been several failed attempts to pass a similar law and each time, the conflict between privacy rights and national security has caused the proposals to be aborted. Additionally, in recent days, the industry has developed huge stakes in processing data and harnessing value from it. Privacy legislation presents a huge hurdle to such business interests.

If the legislation ignores the needs of

all stakeholders and takes into consideration only the views of "privacy activists", the country may not become an "Orwellian State" but is sure to become a "chaotic state" where terrorism will race ahead and business development may significantly suffer.

But is the government becoming a Big Brother? According to Section 35 of the draft PDPB-2019, the central government has retained some powers to exempt itself from all or any of the provisions of this Act. Section 35 deals with the "Power of Central Government to exempt any agency of Gov-



There has been ample criticism of the Bill, even from Justice BN Srikrishna, who headed the committee that drafted it. He, reportedly, said that safeguards had been removed which was most dangerous.



Anthony Lawrence

ernment from application of Act". It says: "Where the Central Government is satisfied that it is necessary or expedient,—

- (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or
- (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

"It may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed."

It is this provision which is being criticised. It may, however, be observed that the Section is drafted clearly to indicate that it is only when the government is satisfied that "it is necessary or expedient" in the "interest of sovereignty and integrity of India, security of the state and friendly relations with foreign states, public order or preventing incitement to the commission of any cognizable offence" that this provision can be invoked. Even in such a case, there has



CONTENTIOUS LEGISLATION
Union minister Ravi Shankar Prasad
defending the Bill in Parliament this month

to be a direction in writing to a specific agency and this would always be available for judicial review.

The reasons under which the provision can be invoked omits “decency or morality or in relation to contempt of court, defamation” which are other reasons provided under Article 19(2) of the Constitution as reasons for which Fundamental Rights can be overridden. The government has, therefore, been restrained in adding this contingent provision and it must be treated as an “enabling provision” which has to be present in the law if the government has to perform its duty to protect citizens.

All privacy and data protection professionals who hail anything foreign may note that even EU General Data Protection Regulation under Article 23 provides similar exemptions. What PDPB-2019 contains is, therefore, reasonable and in tune with the government’s own obligations to society. We should stop nitpicking about whether the safeguards on paper are adequate or not. Details about how this power may be exercised would be in the rules to be notified later and we need to wait for it.

Another area of criticism is the Data Protection Authority (DPA) and whether it would consist of people who are independent and represent the stakeholders. According to Section 42 of the

proposed Act: “The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and specialised knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects.”

The earlier draft had suggested the chief justice of India in the selection panel. This was omitted, giving rise to concerns that the choice of chairman and members could be motivated by the government’s concerns or by the industry lobby. The earlier draft had also suggested maintenance of a “list of five experts”. It is not clear if this was supposed to be an advisory group to guide the DPA and has been omitted.

Industry people know that there is no government secretary who has 10 years’ experience in the field of data protection and is of less than 65 years of age to qualify to be appointed to the DPA. Even in the private sector, there are not many people with such experi-

Data Protection Authority and whether it would have people who are independent and represent the stakeholders is an area of concern. One hopes the government will not bring foreigners and NRIs.

ence who would take up the assignment. So there is a difficulty in the constitution of the DPA.

It is hoped that the government will not look to bring foreigners and NRIs who may have the necessary experience but no commitment to the data sovereignty of India. We can keep our fingers crossed that the right people will be found at the right time for this onerous but responsible position.

The draft also has some positive features which need to be recognised and hailed. One is Section 40 which suggests the creation of a “sandbox” so that startups can benefit by a limited time exemption from the obligations under the Act while they test innovative technologies. Another provision is Section 37 which recognises the need to exempt BPOs in India who only process personal data of foreign citizens on the basis of a contract with a foreign data controller and provide for a suitable notification as may be required. This was necessary for companies maintaining off-shore data processing facilities who needed to comply with data protection laws of the respective countries and would have considered the overlapping of PDPA jurisdiction difficult to manage.

Further, retaining the innovative definition of the role of the “person who determines the means and purpose of personal data” as the “data fiduciary” and the subject as “data principal”, the credit goes to Justice Srikrishna. Additionally, thinking of a role for “consent manager” could be another innovation which the industry will welcome.

To take a balanced view, the Bill has tried to improve upon the earlier version and while fears and concerns are inevitable, they are not completely valid. ■

Twitter: @indialegalmedia
Website: www.indialegalive.com
Contact: editor@indialegalive.com