HERE . NOW
OrissaPOST

FOCUS PRIVACY LAWS

PERILS OF DATA LOCALISATION

Satya Narayan Misra & Kartik Kishore

IN THE AGE OF GLOBALISATION, DATA PROTECTIONISM WOULD BE DETRIMENTAL TO THE ECONOMY

The misuse and arbitrariness of the government would have no bounds if unrestricted access to data is provided to the government

The Government of India, on August 3, withdrew the Personal Data Protection Bill, 2019 (PDP Bill), with a caveat that it would be replaced by a "comprehensive framework" in alignment with contemporary digital privacy laws. Keeping in view the frenetic pace of digitalisation, and vast 'data' resources being created, it is mandatory for India to come up with a robust data protection law. The Supreme Court in the iconic Puttaswamy case (2017), had asked the government to come up with a robust data protection law. Pursuant to this, a report was submitted by Justice Srikrishna Committee in 2018. Responding to the draft bill of the government, Justice Srikrishna observed that the bill will create an Orwellian State. Against this backdrop, some of the provisions of the bill, particularly data localisation, which has stirred the hornet's nest amongst the global intermediaries, Srikrishna Committee recommendations and global practices, need close look and introspection.

The draft law segregates data into personal data, sensitive personal data, critical data, and non-personal data. The most contested issue is the provision of "data localisation," which mandates storing and processing of the personal data of the citizens within the contours of national boundaries. Currently, if India requires access to data that is stored in a foreign nation, Mutual Legal Assistance Treaties (MLAT) is applied. It is an inordinate process, taking more than ten months to get access to information through this mechanism. Often it is even denied. Therefore, Justice Srikrishna Committee had recommended that if the data concerning local people are stored in India itself, it will strengthen the hands of law enforcement agencies.

However, there is a flip side to the application of this policy. The first issue is with the protection of the privacy of the individual. Section 69 of the IT Act, 2000 allows the government to intercept, monitor, or decrypt any information stored in any computer under the garb of reasonable restriction provision in Article 19(2) of the Constitution like sovereignty, integrity, security, and public order of India. The misuse and arbitrariness of the government would have no bounds if unrestricted access to data is provided to the government. Moreover, it may harm the nation economically too. There is a possible threat that foreign companies might opt out of the Indian market. Technological giants like Amazon, Google, and Meta have already expressed their strong displeasure with this law. Their concern is the high compliance cost that they would have to bear to store the data locally. Apart from that, fear also exists on the reaction of the foreign nation to Indian firms operating abroad. In the age of globalisation, data protectionism would be detrimental to the economy.

As alluded to above, in the existing legal dispensation India has to wait for months to get access to data through MLATs. One of the ways to expedite access to data is by establishing a regime of free-flowing data through a bilateral/multilateral framework. It would greatly help India solve the problem of conflicting legal regimes. Moreover, it would also allow Indian law enforcement agencies to easily get access to data stored in a foreign land. The narrative that implementing the policy of restricting data within the boundaries of the nation would allow quick and easy access to any form of data is based on slippery grounds. This is because even if such a policy is implemented, foreign companies would still have to abide by the rules of their home nation. This is especially relevant with US companies that hold most of the world's data. This is analogous to extradition treaties that India has signed with several countries for handing over fugitives, who have committed crimes within the jurisdiction of India.

The Srikrishna Committee which submitted the draft PDP Bill to the government in 2018 had put safeguards on the processing of personal data in the interests of the security of the state. It explicitly stated that it should be authorised pursuant to a law, and must be necessary and proportionate to the interest being achieved. The committee had kept in mind adherence to the Supreme Court's privacy judgement of 2017, which mandates the government to declare a specific objective for collecting private data and what procedure would be followed. However, the Bill that was placed in Parliament by the government has removed those critical safeguards.

While the European Union (EU) came up with the General Data Protection Regulation (GDPR) as a safeguard to data privacy, the US does not follow the tradition of a single overarching privacy law. The US has varied privacy laws based on sectors that work in conjunction with different state privacy and data protection laws. On the other hand, the Russia-China model of data protection is focused on data localisation. In fact, according to the provisions of data localisation laws, websites may be blocked that don't process Russian data in Russia. The biggest drawback of India's draft bill is that there has been no financial viability test as was done while enacting GDPR by the EU. Secondly, the basis for passing of GDPR as discussed by EU members was that it aimed to harmonise the privacy standards throughout the EU. This isn't the case with India. India has the same set of fundamental rights and Right to Privacy which is applicable throughout the nation.

In the age of globalisation, Ricardo's comparative advantage theory of 1817 and free movement of goods and services between countries have brought unprecedented prosperity to all countries. Data localisation on the face of it goes against the spirit of the 'end of geography' as Milton Friedman called it. However, data on wings can be dicey with 'God-like technology' carrying in its womb a dark web and dystopia of politics, commerce and chicanery. The way forward for India is to tread carefully in the matter of data storage and retrieval without losing the benefit of the global commercial network. Data localisation on the lines adopted by the EU and allowing their processing internationally will help the MNCs and intermediaries, which have big stakes in India. Bilateral treaties on data sharing as in the case of extradition treaties will help.

Satya Narayan Misra is Professor Emeritus, KIIT University. Kartik Kishore is Masters in Public Policy, OP Jindal Global University, Sonipat.

www.odishapostepaper.com | All rights reserved © 2022