Source : www.thehindu.com Date : 2019-05-19

WHAT IS INDIA'S STAND ON DATA STORAGE?

Relevant for: Security Related Matters | Topic: Role of Media and Social Networking Sites in internal security challenges

Information Technology background | Photo Credit: bluebay2014/Getty Images/iStockphoto

The story so far: Facebook's Mark Zuckerberg recently expressed apprehension about nations wanting to store data locally. According to him, it gave rise to possibilities where authoritarian governments would have access to data for possible misuse. In an earnings call with investors in late April, he reiterated his stance against data localisation, without mentioning a country. Earlier that month, the U.S. criticised India's proposed norms on data localisation as 'most discriminatory' and 'trade-distortive'. India is at a juncture where various bills are ready to be signed into law that will set data localisation and protection regulations in stone.

Data localisation laws refer to regulations that dictate how data on a nation's citizens is collected, processed and stored inside the country.

Among reasons supporting data localisation put out by the Justice Srikrishna Committee report last year, a few key ones are: Data localisation is critical for law enforcement. Access to data by Indian law agencies, in case of a breach or threat, cannot be dependent on the whims and fancies, nor on lengthy legal processes of another nation that hosts data generated in India.

If data generated in India is stored in the U.S., for example, it is dependent on technology and channels such as the undersea fibre optic cable network. Such reliance can be debilitating in the case of a tech or physical breakdown. The report recommends that hence, at least a copy of the data must be stored in India.

Technology playfields are not even. A developing country such as India may be playing catch-up with a developed nation, which may be willing to offer liberal laws. It may not be wise for India to have the liberal rules as other nations would. A key observation of the report is that it is ideal to have the data stored only locally, without even having a copy abroad, in order to protect Indian data from foreign surveillance.

Currently, the only mandatory rule on data localisation in India is by the Reserve Bank of India for payment systems. Other than this, there are only reports or drafts of bills that are yet to be signed into law.

Among material available in the public domain on data localisation is the white paper that preceded the Jusitce Srikrishna Committee report, inviting public comments.

The second piece is the Draft Personal Data Protection Bill, 2018 itself which has specific requirements on cross-border data transfers. This is seen as being more restrictive than the recommendations of the Srikrishna Committee. The draft e-commerce policy also has clauses on cross-border data transfer. For example, it suggests that if a global entity's India subsidiary transfers Indian users' data to its parent, the same cannot be transferred to a third party even with the user's consent.

The Justice Srikrishna Committee report has made a point about not treating all data alike. For example, a user's reading preferences are not as sacrosanct as his or her Aadhaar details. The data protection bill too differentiates between 'critical' and other data.

The disadvantage for a company compelled to localise data is obvious — costs, in the form of servers, the UPS, generators, cooling costs, building and personnel. Companies feel that infrastructure in India is not yet ready to support this kind of ecosystem. For any large e-commerce player in India, costs may go up between 10% and 50% depending on how stringently the final law is worded. The big daddies of e-commerce and social media may not find it too difficult to comply. Small companies providing services in India will find compliance tough. In fact, one of the objectives of data localisation is to give a fillip to the start-up sector in India, but stringent norms can make it costly for small firms to comply thereby defeating this objective. While this places small entities in a difficult position, the spirit of the Justice Srikrishna Committee report seems to imply that this is not reason enough to avoid compliance.

While granting that the data protection bill comes after a lot of homework, observers feel it is still not comparable to the EU General Data Protection Regulation (GDPR), which took a few years to draft, adding scholarly and academic depth to the consultations, inputs and the final wording of the law.

It is well known that Canada and Australia protect their health data very carefully. Vietnam mandates one copy of data to be stored locally and for any company that collects user data to have a local office, unlike the EU's GDPR; citing national interests, China mandates strict data localisation in servers within its borders. International reports refer to data protection laws in Vietnam and China as being similar, in that they were made not so much to protect individual rights as to allow government to control data.

For the EU, it is clear that customer is 'king'. Their GDPR is agnostic to technology and sector. Interestingly, the U.S. has no single data protection law at the Federal level. It does, however, have individual laws such as the HIPAA (Health Insurance Portability and Accountability Act of 1996) for health care, another for payments, and the like. Brazil, Japan, Korea and New Zealand have put in place data protection laws. Chile has recently announced the setting up of an independent data protection authority, while Argentina is currently reforming its privacy legislation.

In September 2018, the EU had said in its response to India's data protection draft bill that "data localisation requirements appear both unnecessary and potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments". It added that if implemented, "this kind of provision would also likely hinder data transfers and complicate the facilitation of commercial exchanges, including in the context of EU-India bilateral negotiations on a possible free trade agreement".

For companies from one country doing business in another, it becomes cumbersome to have two different compliance levels.

The spokesman said WhatsApp, which has more than 1.5 billion users, immediately contacted Citizen Lab and human rights groups, quickly fixed the issue and pushed out a patch.

The executives at the third-party app makers fear that they are being punished because their apps could be roadblocks on Apple's business growth.

END