A delicate balancing act

The quantum of information that flows across borders has given rise to concerns for national governments. Shagufta Gupta writes that a delicate balancing act is needed to ensure India's digital sector keeps its global lead

Cross-border data flows have engendered a seismic shift in the way the world functions. Consumers and businesses benefit greatly from the free flow of data across borders. For consumers it gives them access to information across the world via the internet, new communication channels have opened to facilitate connectivity across the globe, they have more choice on what they can buy and where they can buy goods and services and the products and services are now more personalised to consumer's tastes.

For businesses cross border data flow opens new markets, provides access to innovative operations solutions at low cost and facilitates cutting edge research and development. India's digital sector has benefited from and leveraged cross border data flows to become not only a leader in Information Technology (IT) and Information Technology enabled Service (ITeS) exports but also a top destination for technology hubs.

India's digital sector has grown phenomenally since its foundation was laid in early nineties. Its size stood at US$413 billion in 2016-17 which was 15-16 per cent of the nation's GDP. The Ministry of Information and Technology estimates it to grow to US$1 trillion by 2025 (18-23 per cent of GDP)[1].

IT and ITeS contribute greater than 60 per cent of this US$413 billion figure. Within IT and ITeS sector, exports constitute a bulk, more than 80 per cent, of the revenue and are growing fast[2].

Enablers of this digital ecosystem, inter alia, include a developing physical infrastructure, availability of relevant skilled workers and conducive policy environment. Additionally, the ability to seamlessly transfer data across borders has been crucial for the sector's growth, which has been primarily driven by exports.

This exponential growth has also consolidated India's position as a top destination for Global Capability Centres (GCCs). Their market size touched US$28.3 billion in 2019, this component of India's digital sector grew even faster

than the IT-ITeS sector over the last four years. More than 1,200 trans-national corporations have their GCCs in India, which employ about a million people[3].

These GCCs are fast developing into centers of innovation and research & development, rising higher in the global value chain, from cost saving centers to strategic and value creation centers. Cross border data flow is an essential component of innovation and research and development and in today's world a critical mechanism of work procurement and delivery as well for these GCCs.

The delicate balancing act required from the Indian government will be the key to sustaining and improving our long-term position in the global digital economy

The explosion of data across the world and the quantum of information that flows across borders has given rise to certain legitimate concerns for national governments.

Issues of privacy and protection of citizens' data, risk of foreign actors accessing data of citizens, national security, law enforcement agencies' (LEA) access to data, spurring of local data economy by promoting local businesses and promoting local innovation are some such issues that nations are grappling with. Data economy has assumed strategic importance and countries are now striving to gain control of this new resource called 'data'.

Various countries have tried to deal with the issues mentioned above in their own ways. Some like US and Japan favor data free flow across borders. These countries were instrumental in promoting the 'Osaka track' on digital economy that was signed by 24 countries and groupings at the G20 summit at Osaka in July 2019.

The declaration supports plurilateral negotiations on digital trade which include data flows, data localisation and cloud computing. Developing countries such as India, China, South Africa and Indonesia opposed this declaration citing the digital divide between developed and developing countries.

According to them, to be able to take advantage of free flow of data, developing countries' digital economy needs to first come to the same level as developed countries. For that to happen, it was necessary for local companies to grow and to be able to compete with global digital companies. Hence, these countries have adopted or seek to adopt a more inward-looking policy on data flows.

With the above mentioned viewpoint the Indian government had introduced the draft Personal Data Protection Bill in 2018[4]. The bill talks at length about privacy, consent and choice issues in the context of the data principals. At the other end it lays out a framework of principles regarding collection and processing of data for the data fiduciaries.

The bill also provides for a national Data Protection Authority to supervise and regulate data fiduciaries. In addition to rights of data principals and obligations of data fiduciaries, the bill requires that a serving copy of personal data be stored within the territory of India, this is referred to as data localization.

The bill also makes it mandatory to store certain critical personal data solely within the country. However, what categorises as personal data and critical personal data has not been unambiguously defined in the bill.

This provision of data localisation has proved to be a highly debated subject in business and policy circles. Sectors such as IT and ITeS exports and GCCs, inter alia, that are dependent on cross border data flows have urged the government to re-strategize; the government at its end is trying to chart the way forward in consultation with stakeholders.

The driving factors behind the Indian government's move towards data localization can be broadly traced to its intention to achieve 'data sovereignty'. Data localisation is believed to assist in this objective via three means.

The first will be by securing the privacy of citizens. If the personal data of citizens are kept within the borders of the country, it would render them less likely to be the subject of unauthorised foreign surveillance. Chances of data breaches by foreign actors, both private and government, will be reduced.

Secondly, ensuring accessibility to law enforcement and regulatory agencies to this data for discharge of their functions will be enhanced due to data localisation.

The third way in which the provision purportedly helps achieve 'data sovereignty' would be via harnessing the latent economic potential in data by local businesses. This would not only open a new sector of data storage for

local businesses but would also lead to more innovation within the country if the locally stored data is processed and analysed by local companies.

There have been many studies across the globe that quantify the economic costs of data localization. One such study by Cory (2017)[5] estimated the cost of barriers to cross border data flow to India (among other countries in his sample) in 2017 at 1-0.7 % of GDP. It is important to bear in mind that the laws governing data localization were not as restrictive and all-encompassing in 2017, as are being proposed in the draft PDP.

The proposed enhanced localization requirement could multiply this cost to the economy. The costs incurred by businesses can arise out of greater compliance costs, reduced efficiency due to disruption of global value chains, increased cost of data storage etc.

India's digital sector is at a particular risk on account of their reliance on cross border data flows not only for their inputs but also as a mode for service delivery. In addition to the economic costs mentioned earlier, there is an increased perceived risk of retaliatory provisions by other countries whose businesses are part of the global digital value chain and might be adversely impacted by data localization requirements in India.

There have been several alternatives suggested that can achieve the objectives cited by the government without disrupting businesses and value chain ecosystems. Privacy and protection of personal data of citizens is more a function of regulatory frameworks in place rather than where the data is stored. The government has proposed to put a privacy and data protection framework in place via the draft bill, by defining the rights of data principals and responsibilities of data fiduciaries.

But its implementation will decide the extent of progress we make in this regard. Having said that, unless the data is completely cut off from outside world it is still prone to attacks by foreign actors in spite of data localization.

In fact, a centralized location is at a greater risk since a single point of failure can lead to entire repository being compromised. Companies distribute their data across different geographical locations to minimize points of failure which will not be possible after data localization.

Other instruments available to ensure data protection are contractual conditions for data processors and adequacy tests for data destinations, as in the European Union's General Data Protection Regulation (GDPR).

Legitimate concerns of law enforcement's and regulator's access to data spring from the failure of currently existing mutual legal assistance treaties (MLATs). These treaties have failed to cut red tape and burdensome protocols and hence have led to huge delays in providing data access to LEAs in critical national security and terrorism related cases. However, data localization which comes at various other costs needs to be carefully weighed against various other options at disposal.

The CLOUD Act of the United States of America provides an alternative framework which does not rely on cooperation of foreign governments. It provides the US government with tools, in the form of warrants or subpoenas, for gaining access to data stored by American companies outside the US jurisdiction.

A balanced response is desired from the government wherein avenues for multilateral cooperation should not be considered closed and should be leveraged to their full potential.

The case for data localization to spur domestic economy and innovation also needs to be revisited. Yes, mandatory localisation would require data storage centers which will increase investment and jobs at least in the initial phases, when the infrastructure is being built. In the long term data centers are almost self-running operations and do not create as many jobs[6]. A careful analysis of jobs gained vs jobs lost will be able to paint a clearer picture.

The second economic argument for data localization stems from the theory that localization will lead to increase in technical and analytical activities by businesses especially by startups, leading to innovation. In addition, access to data will provide them with the fuel that is required to develop Artificial Intelligence and Machine Learning systems.

It could be an important way to bring domestic companies at par with global tech companies. However, this is a protectionist measure that will bring other negative repercussions as part of the deal.

The debate on data localization is highly nuanced and much more involved to be captured in this article. The point that is sought to be made through this piece is that given India's prominent position in the global digital landscape any provision that will shake the ecosystem needs to be carefully evaluated. It is pertinent that the costs and benefits are appropriately studied and alternatives explored before any regulation is passed and implemented.

India's IT and ITeS exports and its position as leading GCC hub is at risk. The lead in this sector that has been painstakingly achieved by our businesses has to be secured. The delicate balancing act required from the Indian government will be the key to sustaining and improving our long-term position in the global digital economy. ■

Shagufta Gupta is a Director at CUTS International & Centre Head, CUTS C-CIER

Endnotes

1. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1565669
2. https://meity.gov.in/content/performance-contribution-towards-exports-it-ites-industry
3. https://timesofindia.indiatimes.com/business/india-business/mnc-tech-hubs-business-in-india-grows-to-28-billion/articleshow/69350843.cms
4. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
5. Cory, N (2017). Cross border data flows: Where are the barriers and what do they cost? Information Technology and Innovation Foundation. Accessed at https://itif.org/publications/2017/05/01/cross-border-data-flows-whereare-barriers-and-what-do-they-cost
6. https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing