Are data localisation requirements necessary and proportionate? Premium

TH thehindu.com/sci-tech/technology/are-data-localisation-requirements-necessary-and-proportionate/article66131957.ece

November 14, 2022

Most countries mandate data created within their borders to remain stored within its borders. Such stringent laws, while allowing governments and their law enforcement agencies to work more efficiently, will result in hindrance of global trade and increase the operational costs of businesses

November 14, 2022 10:30 am | Updated 12:12 pm IST

Nikhil Naren

Data localisation. | Photo Credit: Getty Images/iStockphoto

The importance and use of data in today's technology-driven world is immense. This is understood by both governments and businesses alike. The cross-border data flow has proven to be an important pillar of strength for established as well as growing businesses. The United Nations Conference on Trade and Development in their Digital Economy Report found that businesses using the internet for global trade have a higher survival rate than those who do not. Therefore, it becomes essential for economies [especially growing economies] to protect data during cross-border transfers. Countries mandate data that are created within their borders to remain stored within its

territorial boundaries. This process of storing data locally is referred to as data localisation. The emphasis on the requirement of data localisation has been pressing under the data protection laws of various countries, however with a varying magnitude.

The need for data localisation

The requirement of data localisation strengthens the protection of personal data, as all of us while using the internet are sending data in some manner or form. For instance, obligations under the European Union's General Data Protection Regulation (GDPR), obligates businesses in the EU to keep the data secured within the boundaries of the EU. If in any case such data are to be transferred to a different country, they need to have similar protections like those that exist in the EU. Countries like Russia on the other hand has stricter laws pertaining to the cross-border flow of data and emphasises keeping data within the Russian Federation. What becomes important for us to understand here is that such strict measures may also demotivate businesses to operate in Russia and does not let neither the government nor the businesses cull-out the maximum potential that data could offer. Keeping this in mind, post-Brexit, it was decided that most data could continue to flow from the EU and the European Economic Area without the need for additional safeguards to the U.K. but, in the case of 'restricted transfers', U.K. laws are mirrored as the GDPR. One can, therefore, reasonably infer that the motive for different governments to store data locally is not only to protect the privacy of their citizens but also to exercise their control on the data, which is fuelling and driving businesses in their countries, for law enforcement purposes.

While governments try to reap the most by exploiting data to drive their economy, there are various other challenges that can shoot up due to non-uniform data localisation laws around the globe. Another aspect related to this is the size of the population and subsequently the respective consumer markets. For an effective data localisation framework to be in place, the objectives undertaken by different governments need to be re-assessed to see if there tends to be a uniformity in the nature of data that different businesses operate and exploit.

Also read | The issues around data localisation

India being one of the most powerful markets in terms of data creation and use, the need for data localisation is essential. The recently withdrawn Bill on data protection also emphasised this fact. While some governments may feel that such a move "will serve as a significant barrier to digital trade", there is a necessity of such requirement as law enforcement agencies in India face a lot of difficulties in getting timely access to data that may be stored elsewhere by businesses operating in India. In a similar pattern, due to the increasing number of digital payments in the country, the Reserve Bank of India has also mandated payment system data information to be stored in India for better monitoring and safety.

The flip side

But as it is rightly said, every coin has two sides. The present technology-powered age is impacting trade on a different level. Therefore, imposing restrictions in the free flow of data can not only create an impact on the global economy but also become a hindrance for local markets.

If governments look at data localisation from the point of security and counter data breaches, it can, due to the forced localisation of data, make data security more vulnerable as the data no longer undergoes sharding. This is particularly true of countries with poor IT infrastructure. Moreover, developed countries may use sophisticated tools for data surveillance which can simply forfeit the purpose of achieving data security through relocation. There can also be an increased risk of local surveillance through the implementation of stringent data localisation laws. Additionally, the varied nature of compliances amongst different countries can pose another set of difficulties. For instance, companies using the top-level domain of Kazakhstan (.kz) must function from physical servers located within the country. Malaysia requires consent for international transfer of data and Australia prevents the transfer of identifiable health records outside the country. A lot of countries prohibit transfer of data on the account of 'national interest' which is a very broad term and could encompass various situations. Such variations can foster varied set of challenges in different settings and nature of businesses.

Also read | What next on data protection?

Further, the mandate of data localisation increases the operational costs of the businesses. Another downside of this could be promotion of monopoly and eradication of small and mid-size businesses from the market. Therefore, the impact is not only felt by these businesses but also by the daily consumers who would be deprived of making choices when they wish to avail these services or purchase goods. Secondly, the nature of automation followed in the data centres that are set up to store data locally, does not foster employment opportunities but instead incurs high investment and energy costs.

A multiple stakeholder approach

Data is the enabler of businesses and digitisation that has been essential for growth and innovation. In this age of rapid technological growth, governments should shift to alternate standards (such an encryption) rather than enforcing strict measures on data localisation that could restrict trade and innovation. One should also reflect on how far we can go with a sovereignty-based model in a digitally connected world. It has become increasingly troublesome to solve jurisdictional issues in case of cybercrimes and online defamation which rely heavily on international cooperation between countries, making it difficult and expensive for prosecutors to act. Therefore, a way forward could be to move with a multiple stakeholder approach which can not only help in looking at data localisation alone, but also other issues such as privacy and governance.

The ‘glocalization’ approach is one such method in the digital space, wherein laws can be harmonised globally, but by paying attention to local interests. Last but not the least, with the pressing need for data localisation by the governments, it becomes important to assess the security of domestic systems for storing sensitive data. There is no denying the fact that robustness of IT systems should become more important than the geographical location of data storage.

Nikhil Naren is Assistant Professor at Jindal Global Law School, a British Chevening Scholar, an Author, and Of Counsel at Scriboard, New Delhi.