Data localisation norms can hurt a nation's GDP

The Reserve Bank directive relating to the payment industry could impact the vision of cashless India

If the 20th century brought the promise of the Internet as a decentralised and self-regulating space, the 21st century is marked by battles over the control of data. There are many permutations in data localisation laws; however, they require data to be processed within a particular territory or country as opposed to in a cloud. Apart from storage, regulations might also restrict data from being transmitted outside a territory. Many countries have announced or have already put in place data localisation norms: Vietnam, Indonesia, Brunei, Iran, China, Brazil, India, Australia, Korea, Nigeria and, most recently, Russia.

These regulations are alarming for several reasons. First, it increases cost for companies. Second, data localisation restrictions can negatively impact GDP of countries mandating it. Third, such policies often seen as a tool to enable local surveillance. Fourth, they also increase the cyber vulnerability and restrict access of SMEs to global services.

Data localisation laws often do not mandate a blanket localisation of data. Europe's new data protection regime does not introduce localisation requirements but instead puts limits on cross-border data flows to countries that don't have data protection laws.

In 2017, the government constituted the Justice BN Srikrishna committee to draft a data protection law. While the panel is yet to finalise its recommendations, the Reserve Bank of India, in April, stated that "all system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India". Their objective is to ensure "unfettered supervisory access to data stored with these system providers as also with their service providers/ intermediaries/ third party vendors and other entities in the payment ecosystem".

The goal of access to data is understandable from the regulator's perspective; however, there are better mechanisms to achieve this. Importantly, once India has a robust data protection law in place, personal data of Indian residents, wherever stored, will be bound to comply with requirements of ensuring security and access to data by law enforcement and users. However, in the context of the RBI directive for payment system operators, ironically most of them do not see or store the personal data of consumers. The Reserve Bank of India directive without any industry consultation will undermine the required support from the global industry to achieve the vision of a cashless India. Increased compliance cost and additional reporting requirement will foresee a decrease in investment in the payment industry in India.

Sudhir Gupta is former secretary, TRAI, and honorary principal adviser, Broadband India Forum. Kaushal Mahan is a technology policy analyst. The views expressed are personal