Source : www.indianexpress.com Date : 2019-07-30

GOING LOCAL

Relevant for: Developmental Issues | Topic: E-governance - applications, models, successes, limitations, and potential incl. Aadhaar & Digital power

A high-level government panel has recommended doing away with the requirement of foreign firms needing to store a copy of all personal data within India. Firms will now be able to store and process data abroad, though critical personal data will have to be processed and stored in the country. This approach marks a significant departure from the recommendations of the Justice Srikrishna committee report which had suggested that a copy of personal data must be stored in the country. The panel's decision comes after a rethink by the Reserve Bank of India, which earlier relaxed its April 2018 circular that had mandated that all payment data generated in the country be stored here. This decision, which is likely to be welcomed by foreign companies, who would have seen a surge in costs to comply with these regulations, suggests that a more considered view on localisation norms is evolving in India.

The arguments in favour of data localisation are straightforward — it will address questions on privacy and security, enable greater governmental access to data, and help develop local data infrastructure. But on each of these issues, it is not very clear if the benefits from localisation outweigh the costs. For instance, in the absence of a strong data protection law, questions of privacy and security are unlikely to be addressed. And while there are reasonable arguments to be made in favour of law enforcement having greater access to data, especially when it is not stored in India, interventions such as bilateral treaties aimed at addressing specific issues might be a more prudent approach. This is not to suggest that localisation is never acceptable. There may be cases when it is justified. But these require careful cost-benefit analysis.

The next set of questions are likely to centre around what constitutes critical personal data. The Srikrishna committee report had classified personal data pertaining to finances, health, biometric and genetic data, religious and political beliefs, among others, as sensitive personal data. It had envisaged a data protection agency which would list out further categories of sensitive personal data. But it is debatable whether a single agency is best suited to draw up this list. As, globally, the framing of localisation norms has been largely contextual, driven typically by the type of data and the sector it relates to — in Canada, any data may be sensitive based on the context — sector specific regulators might be better at identifying which data is sensitive.

END