Payment Firms Begins Process of Data Localisation

Global card payment companies like Visa and MasterCard have started to comply with the Reserve Bank of India's (RBI) norms on data localization.

- The **RBI gave October 15 as the deadline for global financial technology** companies to comply with its data localization norms in India and to store transaction data of Indian customers within India.
- In a circular in April 2018 RBI said 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.
- This covered not only card payment services by Visa and MasterCard but also of companies such as Paytm, WhatsApp and Google which offer electronic or digital payment services.
- This data includes the full end-to-end transaction details/ information collected/carried/processed as part of the message/payment instruction.
- **RBI's directives were followed by the draft data protection law recommended by the Srikrishna committee.**

What is Data Localisation?

- Data localization is the **practice of storing data on any device that is physically present within the borders of the country** where the data is generated. As of now, most of these data are stored, in a cloud, outside India.
- Localization mandates that companies collecting critical data about consumers must store and process them within the borders of the country.

Importance of Data Localisation

- The main intent behind data localization is to **protect the personal and financial information of the country's citizens and residents** from foreign surveillance like social media giant Facebook sharing user data with Cambridge Analytica, which is alleged to have influenced voting outcomes.

- It gives **local governments and regulators the jurisdiction to call for the data when required.** This aspect has gained importance after a spate of lynchings across States which was linked to WhatsApp rumor.
- RBI has said that unfettered access to data stored by system providers and third-party vendors in the payments ecosystem will ensure better monitoring.
- **Data localization is essential to national security.** Where data is not localized, the agencies need to rely on mutual legal assistance treaties (MLATs) to obtain access, delaying investigations.
- On-shoring global data could also create domestic jobs and skills in data storage and analytics too.
- Global service providers like Facebook and Google collect all sorts of data about its consumers. It is necessary to have greater accountability from these firms about the end-use of the data.
- **India's one billion-strong consumer market prove to be a stronger bargaining chip when it comes to pushing for data localization.**

Issues with respect to Data Localisation

- Maintaining multiple local data centers may lead to **significant investments in infrastructure and higher costs for global companies.**
- One of the argument is that localization will help in enhancing data security. But, by storing data at multiple locations, service providers enhance their data security in case of a breach at one location.
- The impact of data localization on the **economy and on data-driven innovation will be highly negative.** European Centre for International Political Economy - ECIPE 2014 Study has estimated GDP loss of 0.8%, reduced growth by 20%, decrease in FDI by 1.9%. World GDP grew by 10.1% on account of trade of $7.8 trillion – out of which data flows account for $2.8 trillion (Mckinsey Study 2016) and India's share is a mere $175 billion.

- Clouds and large service providers implement risk-based security programs that track the latest threats and vulnerabilities, with the latest technology tools, and highly skilled manpower. **Small organizations can not invest that much for security, while the risks are similar.** The norms should not discourage that since India as the global hub of IT/BPM industry is home to such data processing.

Way Forward

- Data localization may not entirely avoid Facebook-Cambridge Analytica-like episodes but it can ensure that domestic law enforcement can respond more effectively to such issues.

- It is said that data localization will help avoid the vulnerabilities of relying on the fiber optic cable network. The Cyber Security Report 2017 released by Telstra reported that businesses in India were most at risk to cybersecurity attacks. Thus, a mandatory border control provision may not be the solution to avoiding security breach incidents. Instead, using superior encryption and adoption of robust security measures will help to prevent the security breach.

The **Justice Srikrishna Committee Report** and the **Personal Data Protection Bill, 2018** (Data Protection Bill) has proposed:

- all personal data to which the law applies must have at least one serving copy stored in India
- personal data critical to national interest must be stored and processed only in India
- the Centre will have the power to exempt transfers on the basis of strategic or practical considerations.