Data Localisation

Why in News?

- 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 had 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.

Background

Srikrishna Committee Report

- Atleast one copy of personal data will need to be stored on servers located within India.
- Transfers outside the country will need to be subject to safeguards.
- Critical personal data will only be stored and processed in India.

Data Protection Bill 2018

- The right to privacy is a fundamental right which necessitates protection of personal data as an essential facet of informational privacy.
- Establishment of a Data Protection Authority to take steps to protect interests of individuals, prevent misuse of personal data and to lay down norms for cross-border transfer of personal data.
- The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

Draft National E-Commerce Policy Framework

- Recommended data localisation and suggested a two-year sunset period for the industry to adjust before localization rules becomes mandatory.
- Proposes incentives to encourage data localization and grant infrastructure status to data centres.

What Is Data Localisation?

- Data localisation 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.
- Localisation mandates that companies collecting critical data about consumers must store and process them within the borders of the country.

Advantages of Data Localisation

- Secures citizen’s data and provides data privacy and data sovereignty from foreign surveillance. Example - Facebook shared user data with Cambridge Analytica to influence voting.
- Unfettered supervisory access to data will help Indian law enforcement ensure better monitoring.
- Ensures National Security by providing ease of investigation to Indian Law Enforcement agencies as they currently need to rely on Mutual Legal Assistance Treaties (MLATs) to obtain access to

data.
- It will give local governments and regulators the jurisdiction to call for the data when required.
- Data centre industries are expected to benefit due to the data localisation which will further create employment in India.
- Greater accountability from firms like Google, Facebook etc. about the end use of data.
- Minimises conflict of jurisdiction due to cross border data sharing and delay in justice delivery in case of data breach.

NOTE: Mutual Legal Assistance Treaties (MLATs) are agreements between governments that facilitate the exchange of information relevant to an investigation happening in at least one of those countries.India has signed Mutual Legal Assistance Treaty (MLAT) with U.S. and 39 other countries.

Challenges of Data Localisation

- Maintaining multiple local data centres may lead to significant investments in infrastructure and higher costs for global companies.
- Infrastructure in India for efficient data collection and management is lacking.
- Splinternet or 'fractured internet' where the domino effect of protectionist policy can lead to other countries following suit.
- Even if the data is stored in the country, the encryption keys may still remain out of the reach of national agencies.
- Forced data localisation can create inefficiencies for both businesses and consumers. It can also increase the cost and reduce the availability of data-dependent services.

International Practices

- Many countries have implemented or are in the process of implementing data localisation laws, including — China, United States, Brazil, Indonesia and Russia.
- Europe's new data protection regime puts limits on cross-border data flows to countries that don't have data protection laws.

Way Forward

- There is need to have an integrated long-term strategy for policy creation for data localisation.
- Adequate infrastructure and adequate attention need to be given to the interests of India's Information Technology enabled Services (ITeS) and Business Process Outsourcing (BPO) industries, which are thriving on cross border data flow.