

## General Studies-3; Topic- Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges

### Data Localisation in India

#### 1) Introduction

- Data localisation refers to the process of storing data within the borders of a particular country where the data was generated.
- If the 20th century brought Internet as a decentralised space, the 21st century is marked by battles over the control of data.

#### 2) Need for Data Localisation

- For securing citizen's data, data privacy, data sovereignty, national security, and economic development of the country.
- Much of the data from online sales, on ecommerce platforms is likely to be hosted and stored in US data firms.
- The extensive data collection by technology companies, has allowed them to process and monetise Indian users' data outside the country.
- To curtail the perils of unregulated and arbitrary use of personal data
- With the advent of cloud computing, Indian users' data is outside the country's boundaries, leading to a conflict of jurisdiction in case of any dispute.
- Data is a digital transactions footprint. During war or hostilities, data centres could be switched off. Such scenarios are pushing countries towards local infrastructure.

#### 3) Advantages

- Data centre industries are expected to benefit due to the data localisation.
- It will speed up transactions and reduce network latency.
- When an online grocery store shifted its data centre from Singapore to Mumbai, it noticed up to 10 per cent improvements in transaction efficiency.
- The manpower, real estate and bandwidth costs come down by about 80 per cent compared to a top-tier data centre in the US or Singapore.
- It is also likely to help IT and telecom infrastructure players grow.
- This is an opportunity for Indian technology companies to evolve an outlook from services to products.
- More data centres in India could mean new, power-hungry customers for India's renewable energy market. That means Data localisation could boost India's renewable energy.

#### 4) Arguments for Data Localisation

- Data localisation will help Indian law enforcement agencies access data.
- RBI circular says that, it is important to have unfettered supervisory access to data stored in India.
- Recently lynching across the country were linked to WhatsApp rumours and in this context, localisation of data assumes significance.
- It gives security against foreign attacks and surveillance.
- Domestic companies support data localisation citing examples of China and Russia.
- Data is the new oil, data is strategic and foreign entities could cripple India in event of war or sanctions.
- India's data localisation push can give rise to new business opportunity.

- India is an ideal location for lower cost of operations and availability of quality talent.
- National wealth creation relies on in-house data storage.
- It champions domestic innovation.
- Massive amounts of data generated by cities can be used to improve infrastructure and transport systems as Singapore has done.

### 5) Arguments against Data Localisation

- It will create domino effect of protectionist policy and other countries may also follow it. This leads to fragmentation of internet.
- US-India Business Council is also against Data localisation.
- It may affect India's young start-ups that are attempting global growth.
- It may affect big firms like TCS and Wipro because they are processing foreign data in India.
- Even if the data is stored in the country, encryption keys may remain out of reach of national agencies.
- It can act as "barriers" to expansion of services in India, impacting not only consumers but also growth of Indian payments market.
- Infrastructure in India for efficient data collection and management is lacking.

### 6) Recommendations for Data Localisation

- Reserve Bank of India (RBI) has firmly stated that all financial transactions' data must be locally stored.
- Data protection draft law by Justice B N Srikrishna recommended that all personal data of Indians should have at least one copy in India. Critical personal data must be stored and processed only in India.
- Draft of the e-commerce policy indicates localisation for community data generated by users in India through various e-commerce platforms, social media and search engines.
- Draft report on cloud computing recommended localisation of data.

### 7) International Practice

- Many countries have implemented or are in the process of implementing data localisation laws, including — China, United States, Brazil, Indonesia and Russia.
- Russia has the most restrictive regulation for data flows with strict localisation.
- Europe's new data protection regime puts limits on cross-border data flows to countries that don't have data protection laws.
- China mandates localisation for all important data held by critical information infrastructure and any cross-border personal data transfer must undergo a security assessment.
- US President Donald Trump signed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which established data sharing with certain countries.
- European Centre for International Political Economy found a surge in data localisation measures worldwide over the last decade.

### 8) Way Forward

- There is an urgent need to have an integrated, long-term strategy for policy creation for data localisation.
- Devising an optimal regulatory and legislative framework for data processors and data centres operating in the country.

- Adequate infrastructure in terms of energy, real estate, and internet connectivity also needs to be made available for India to become a global hub for data centres.
- Adequate attention needs 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
- Data needs to be shared with start-ups so that they can have a level playing field in offering innovative services with large and often global data companies.

