Data Localisation

Last Updated: August 2022

For Prelims: Data Protection, Personal Data, Privacy, Personal Data Protection Bill, Data Localisation, Other Related Laws.

For Mains: Data localisation: Advantages, regarding concerns, provisions in India, Global practices, steps that can be taken.

Why in News?

- The government of India has withdrawn the **Personal Data Protection Bill** from **Parliament** as it considers a **"comprehensive legal framework"** to regulate the online space to boost innovation in the country **through a new bill.**
    - Technology giants like **Facebook and Google are against it** and have criticised the protectionist policy of **data localisation** as they are afraid it would have a domino effect in other countries as well.

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.
- The most important aspect of data localisation is having control over our own data which makes the country **more resistant to issues around privacy, information leaks, identity thefts, security etc.**

Data Localisation and India: What is the Scenario?

- **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.

- **Boycott of Osaka Track**:
    - At the **G20 summit 2019,** India boycotted the **Osaka Track on the digital economy.** The Osaka Track pushed hard for the creation of laws that would allow data flows between countries and the removal of data localisation.

What are the Advantages of Data Localisation?

- **Protects Privacy and Sovereignty:** Secures citizens' data and provides data privacy and data sovereignty from foreign surveillance.
    - Example - Facebook shared user data with Cambridge Analytica to influence voting.
- **Monitoring of Laws & Accountability:** Unfettered supervisory access to data will help Indian law enforcement ensure better monitoring.
    - Data localisation will result in **greater accountability from firms** like Google, Facebook etc. about the end use of data.
- **Ease of Investigation:** 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.
    - 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.
- **Jurisdiction & Reduction in Conflicts:** It will give local governments and regulators the jurisdiction to call for the data when required.
    - Minimises conflict of jurisdiction due to cross border data sharing and delay in justice delivery in case of data breach.
- **Increase in Employment:** Data centre industries are expected to benefit due to the data localisation which will further create employment in India.

What are the Challenges Regarding 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.

What are the Global Practices Regarding Data Localisation?

- **Canada and Australia** protect their health data very carefully.
- **Vietnam** mandates one copy of data to be stored locally and for any company that collects user data to have a local office citing national interests
- **China** mandates strict data localisation in servers within its borders.
- **The** European Union (EU) had enacted the **General Data Protection Regulation (GDPR)** which establishes the right to privacy as one of the fundamental rights. It requires explicit consent from consumers for usage of their data.
- **The United States** has no single data protection law at the Federal level. It does, however, have individual laws such as **HIPAA (Health Insurance Portability and Accountability Act of**

1996) for health care, another for payments, and the like.

What can be the 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.
- **Data localisation is critical for law enforcement.** Access to data by Indian law agencies, in case of a breach or threat, cannot be dependent on the whims and fancies, nor on lengthy legal processes of another nation that hosts data generated in India.
- India needs to work out a way to crack cyber frauds and crimes. For this, the country urgently **needs a legally backed framework for a collaborative trigger mechanism** that would bind all parties and enable law enforcers to act quickly and safeguard Indian citizens and businesses from a fast-growing menace.
- All the players involved, including banks, telecom companies, financial service providers, technology platforms, social media platforms, e-commerce companies and the government, **need to play a responsible role** in ensuring innocent citizens do not undergo the trauma of suffering losses.
- The customer also has a responsibility to **maintain basic cyber hygiene,** which includes following practices and taking precautions to keep one's sensitive information organized, safe and secure.