Data Localisation

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, Steps that can be taken

Why in News?

Recently, the United Nations Conference on Trade and Development (UNCTAD) highlighted the importance of Data Localisation for economies to protect data during cross-border transfers.

- The UNCTAD in its report found that businesses using the internet for global trade have a higher **survival rate than those who do not.**

What is Data Localisation?

- Data Localisation is storing critical as well as non-critical data within the territorial boundaries 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.
    - It has also helped the countries develop their own **startups, evolve locally and also thrive** in their own language.

What are the Advantages of Data Localisation?

- **Protects Privacy and Sovereignty:**
    - Secures citizens' data and provides **data privacy and data sovereignty** from foreign surveillance.
    - The main intent behind data localisation is **to protect the personal and financial information** of the country's citizens and residents from foreign surveillance
- **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 a **Mutual Legal Assistance Treaty (MLAT) with 45 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 center industries are expected **to benefit due to localisation** which will further create employment in India.

What are the Disadvantages of Data Localisation?

- **Investments:**
    - Maintaining multiple local data centers may lead to significant investments in infrastructure and higher costs for global companies.
- **Fractured Internet:**
    - Splinternet, where the domino effect of protectionist policy can lead to other countries following suit.
- **Lack of Security:**
    - Even if the data is stored in the country, the encryption keys may still remain out of the reach of national agencies.
- **Impact on Economic Growth:**
    - 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 Data Localisation Norms?

- **In India:**
    - **Srikrishna Committee Report:**
        - At Least 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.
    - **Personal Data Protection Bill, 2019:**
        - The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, on December 11, 2019.
        - It intended to **protect individual rights by regulating the collection, movement,** and processing of data that is personal, or which can identify the individual.
        - This bill was though withdrawn from Parliament in 2022 as government considers a **"comprehensive legal framework" to regulate the online space to boost innovation in the country** through a new bill.
    - **Draft National E-Commerce Policy Framework:**
        - Recommended data localisation and suggested a two-year sunset period for the industry to adjust before localization rules became mandatory.
        - Proposes incentives to encourage data localization and grant infrastructure status to data centers.
    - **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.
    - **Banning of Chinese Mobile Apps:**
        - In 2020, the Indian government announced to ban 59 widely used apps (such as Tik Tok, ShareIt, Cam scanner etc), most linked to Chinese companies.
        - The Ministry of Electronics and Information Technology (MeitY), invoked Information Technology (IT) Act, 2000 to cite the concerns regarding both data security and national sovereignty associated with these apps.
- **Global:**
    - **Canada and Australia** protect their health data very carefully.

- **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.
- **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.
- Many bilateral and multilateral agreements exist as well. These include countries committing to identical data protection norms and commitments towards cross-border data transfer and data localisation, examples being, **the** Clarifying Lawful Overseas Use of Data (CLOUD) Act (2018), Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018), Digital Economy Agreement (DEA), (2020), among others.

Way Forward

- There is a need to have an **integrated long-term strategy** for policy creation for data localisation.
- 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.
- 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.
    - According to the sources, lack of law enforcement is causing issues in the recent Free Trade Agreement (FTA) between India and UK.
- 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.

Source: TH