Data Localisation and Undivided Internet

This editorial is based on the article "What is India's stand on data storage?" which appeared in "The Hindu" on 18th May, 2019. The article talks about the need and the implications of Data-localisation.

Why in News?

- Facebook's Mark Zuckerberg recently expressed apprehension about nations wanting to store data locally. According to him, it gave rise to possibilities where authoritarian governments would have access to data for possible misuse.
- Moreover, U.S. criticised India's proposed norms on data localisation as 'most discriminatory' and 'trade-distortive'. India is at a juncture where various bills are ready to be signed into law that will set data localisation and protection regulations in stone.

What is Data Protection?

- Data localisation laws refer to regulations that dictate how data on a nation's citizens is collected, processed and stored inside the country.
- In India, data localisation law requires that data be stored and processed physically within the territory of India.

Which Sectors Already Have Data Localisation Requirements?

- Mandatory rule on data localisation in India has been placed by the **Reserve Bank of India** for payment systems.
- **Telecom:** where telecom companies are required under their licence terms to store "user information" only in India. The Indian government isn't unique in this belief – countries such as Germany have similar restrictions in the telecom sector.
- Apart from telecom, there are limited data localisations requirements in just a few other sectors such as **insurance (details of policies and claims are to be stored only in India) and banking (where certain original records need to be maintained in India, though there is no bar on transfers of copies outside)**.

What are the Policies in India on Data-localisation Laws?

- **Justice Srikrishna recommendation on data protection**
  - The committee has proposed strict standards for cross-border transfer of data and storage.
  - Critical personal data, to be notified by the government, must be stored and processed at a data centre located in India.
  - Personal data can be transferred outside India but will need to comply with conditions of security, purpose limitation, storage limitation, data principals' rights as laid down under the Indian law.
  - Every **data fiduciary** will need to store at least one serving copy of personal data on a server or data centre located in India.
- **Draft Personal Data Protection Bill, 2018 which has specific requirements on cross-**

border data transfers.
- The draft e-commerce policy also has clauses on cross-border data transfer.

Why Data Localisation is Important?

- To protect the personal and financial information of the country's citizens and residents from **foreign surveillance** and give local governments and regulators the jurisdiction to call for the data when required.
- Storing of data locally is expected to **help law enforcement agencies** to access information that is needed for the detection of a crime or to gather evidence. This gets significant importance due to increasing relevance of technology in nature as well as the resolution of crimes.
- 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, as the Srikrishna report had pointed out.

Why are Companies Reluctant to Comply?

- **High costs-**costs, in the form of servers, the UPS, generators, cooling costs, building and personnel and carious physical and infrastructural costs.
- **IT infrastructure:** Companies feel that infrastructure in India is not yet ready to support this kind of ecosystem. For any large e-commerce player in India, costs may go up between 10% and 50% depending on the provisions of final law.
- Small companies providing services in India will find compliance tough. In fact, one of the objectives of data localisation is to give a fillip to the start-up sector in India, but stringent norms can make it costly for small firms to comply thereby defeating this objective.

Is Location Sole Measure of Claiming Data Rights?

Some provision of cross-border data sharing conundrum can be solved by the **CLOUD Act** passed by the US congress are as following.

- The Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed by the U.S. Congress earlier last year, seeks to de-monopolize control over data from U.S. authorities.
- The law will for the first time allow tech companies to share data directly with certain foreign governments.
- This requires an executive agreement between the U.S. and the foreign country certifying that the state has robust privacy protections and respect for due process and the rule of law.
- The CLOUD Act creates a potential mechanism through with countries such as India can request data not just for crimes committed within their borders but also for transnational crimes involving their state interests.

Data-localisation and Splinter-net

- Data localisation is undoubtedly a problem on the face of the idealised conception of the internet as a borderless world.
- And though this idea of the borderless internet has lost some of its sheen in recent years, it's hard to deny that it has been one of the main reasons for explosive digital growth. Online services can spread and scale across dozens of countries without having to set up physical infrastructure in more than a few.
- Additionally, the ability to aggregate data and derive value from it is a key value proposition for many internet businesses, and data localisation jeopardises that model.
- Major Indian start-ups, benefited from this borderless world which allows them to offer their services in new countries while still largely operating their digital infrastructure out of just one, with reduced infrastructure and compliance cost.
- A fragmented internet, or **"splinternet"**, is not a friend to permission less innovation and would be at odds with the goal of India as a major digital power.

Way Forward

- Policymakers must believe in the transformative power of Indian entrepreneurs to succeed globally and allow those entrepreneurs to sit at the table and be part of decisions regarding privacy and data flows.
- Incorporation should also be made from EU's **Data Transfer model and the CLOUD Act**.

Data Transfer Model

- This model has been successfully adopted by the EU, which allows for data transfer upon review and approval of a company's data processing policies by the relevant Data Protection Authority.
- Through this process, user rights are protected, data is secured, and companies can still do business.
- By giving all Indian companies the benefits of data transfer the Indian industry will likely be able to expand globally with fewer policy obstacles.

Drishti Input:

Data localisation is undoubtedly a wrinkle on the face of the idealised conception of the internet as a borderless