Are data localisation requirements necessary and proportionate?

By IASToppers | 2022-11-16 17:25:00

Are data localisation requirements necessary and proportionate?

With increase in cross border transaction, recently there has been an upheaval in the world governments to opt for data localisation.

[*Ref: The Hindu*]

Data Localisation:

- Data localization is the **practice of keeping data within the region it originated from.**
- **Data residency** refers to the place **where data is stored.**
    - Data residency requirements may compel organizations to change where their data resides.
- Data localization is the action of complying with data residency requirements.

Need for data localisation:

- The requirement of data localisation **strengthens the protection of personal data**, as all of us while using the internet are sending data in some manner or form.
- For instance, obligations under the European Union's General Data Protection Regulation (GDPR), obligates businesses in the EU to keep the data secured within the boundaries of the EU.
    - If in any case such data are to be transferred to a different country, they need to have similar protections like those that exist in the EU.
- Countries like Russia on the other hand has stricter laws pertaining to the cross-border flow of data and emphasises keeping data within the Russian Federation.

Arguments in favour of stringent data localisation norms:

- **Sovereignty and government functions**; referring to the need to recognise Indian data as a resource to be used to further national interest (economically and strategically), and to enable enforcement of Indian law and state functions.
    - It would be easier for law enforcement agencies to access information within their jurisdiction as compared to waiting for responses to requests made to foreign entities which store data abroad.
- The **economic benefits** will accrue to local industry in terms of creating local infrastructure, employment and contributions to the AI ecosystem.
- The local hosting of data will **enhance its privacy and security** by ensuring Indian law applies to

the data and users can access local remedies.

- **Avoiding resultant vulnerabilities of relying on fiber optic cable network:**
  - A large amount of data is transmitted from one country to the other via undersea cables.
  - The **location** of almost every **undersea cable in the world is publicly available**, which increases the risk of vulnerability of the internet and cross-border transfer of data.
- **Cost of data protection trumps:**
  - All or most **legal obligations** give rise to **economic costs** for regulated entities and thus mere increase in costs cannot be reason not to introduce legal change.
  - Rather, it must be shown that the costs incurred due to rules demanding local processing outweigh the benefits of such a requirement.
- **Building an AI ecosystem:**
  - In the coming years AI is expected to become pervasive in all aspects of life that are currently affected by technology and is touted to be a major driver of economic growth.
  - The benefits that developing countries can derive from a policy of data localization are:
    - Higher foreign direct investment in digital infrastructure;
    - The positive impact of server localization on creation of digital infrastructure and digital industry through enhanced connectivity and presence of skilled professionals.

Creation of digital industry and digital infrastructure are essential for developments in AI and other emerging technologies, therefore highlighting the significance of a policy of requiring either data to be exclusively processed or stored in India.

Arguments against Data Localization:

- **Data versus Data Center – Jurisdiction:**
  - Access to data depends on who has custody, control and possession of the actual data and that may not necessarily be with the entity that provides the local hosting facility.
- **Data Localization cannot stop foreign surveillance:**
  - Several foreign governments are reported to use **sophisticated malware for data surveillance.**
  - Thus, physical access to the data storage or processing facilities is not technically necessary in order to conduct surveillance activities.
- **Threat of domestic surveillance:**
  - The local government may exercise greater coercive power over domestic businesses storing data to circumvent legal protections.
- **Cost of localization:**
  - Reports suggest that the **costs of effecting the data localization requirements are prohibitive.**
  - As per study, data localization measure raises cost of hosting data by nearly 30 % to 60%.
- **Cost of data breach:**
  - **Revenue leakage** will be unavoidable during the transition from the present set-up to a new regime.
  - The **2018 Cost of a Data Breach:** Global Overview study reports that the global average cost of data breach is already up to 6.4 percent over the previous year to USD 3.86 million.
  - The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent per year over to USD148.

Way Forward:

- Governments should **shift to alternate standards** rather than enforcing strict measures on data localisation that could restrict trade and innovation.
- A **multiple stakeholder approach** is needed which can not only help in looking at data localisation alone, but also other issues such as privacy and governance.
- The '**glocalization'** approach is one such method in the digital space, wherein laws can be harmonised globally, but by paying attention to local interests.
- The **robustness of IT systems should become more important** than the geographical location of data storage to assess the security of domestic systems for storing sensitive data.
- For an effective data localisation framework to be in place, the objectives undertaken by different governments need to be re-assessed to see if there tends to be a uniformity in the nature of data that different businesses operate and exploit.

