Cyber Crime: Data Deprivation and Data Localisation

The article is based on “Data deprivation makes cybercrime difficult to tackle” that was published on 22nd August in Livemint. It talks about the challenges in tackling Cyber crimes due to Data deprivation and the need of Data Localisation.

Context

- In recent times, there have been many instances of the hard-earned money of Indians being taken out of bank accounts and charges loaded onto credit cards through online frauds.
- These cyber crimes shake people’s faith in digital systems. The scepticism vis-a-vis online transactions also hurts the potential of emerging companies, tomorrow’s successes which could help take India to the $5 trillion economy that the country aspires to.
- While many cases aren’t even reported, in cases that are, the investigations make little or no progress due to **lack of access to data** because of data possessing entities try to take cover under privacy principles or laws of the countries they are based in.
- Since most search engines and social media platforms have no “permanent establishment" in India, law enforcement agencies have hit a wall on data access for the purpose of solving cyber crimes.This has often raised calls for complete **data localization**, which could have been avoided had a collaborative mechanism for data access, based on agreed criteria, been put in place.
- Revelations of social media giant Facebook, sharing user data with Cambridge Analytica, which is alleged to have influenced voting outcomes, have led to a global clamour by governments for data localisation.

Data Localisation

- Data localisation is the **act of storing data** on any device **physically present within the borders of a country.**
- Data localisation laws refer to regulations that dictate how data on a nation’s citizens is collected, processed and stored inside the country.

Need for Data Localisation

- The main intent behind data localisation is **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.**
- Data localisation is **essential to national security.** 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.
- Where data is not localised, 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, as the Srikrishna report had pointed out.

Data Localisation and India

- **The Srikrishna Commission** recommended that data be stored in the country either directly or through mirror servers to serve law enforcement needs.
- **The Reserve Bank of India** imposed a hard data localisation mandate on payment systems providers to store payment systems data only in India.
- The **draft e-commerce policy** also has clauses on cross-border data transfer. For example, it suggests that if a global entity's India subsidiary transfers Indian users' data to its parent, the same cannot be transferred to a third party, even with the user's consent.
- **Draft Personal Data Protection Bill, 2018** has specific requirements on cross-border data storage.
    - The Bill states that every fiduciary shall keep a 'serving copy' of all personal data in a server or data centre located in India.
    - The central government may notify certain categories of personal data as exempt from this requirement on grounds of necessity or strategic interests of the State.
    - The central government may also notify certain categories of personal data as 'critical personal data', which may be processed only in servers located in India.
- At the **G20 summit 2019**, India boycotted the **Osaka Track on the digital economy.** The Osaka Track pushed hard for the creation of laws which would allow data flows between countries and the removal of data localisation.

Global Practices Regarding Data Protection

- **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 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 U.S.** 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.

Concerns Regarding Data Localisation

- **Oppositions from Global Internet Giants:** 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.
- **Opposition from US:** The US Electronic Communications Privacy Act bars US-based service providers from disclosing electronic communications to law enforcement agencies of any country unless US legal requirements are met.
    - The U.S. criticised India's proposed norms on data localisation as 'most discriminatory' and 'trade-distortive'.
- **EU concerns:** termed data localisation as unnecessary and potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments.
- The bilateral mechanism of the India-US Mutual Legal Assistance Treaty is a bit outdated and does not seem to work. The US Cloud (Clarifying Lawful Overseas Use of Data) Act, however, enables law enforcement authorities in India to request electronic content directly from US service providers under an executive agreement with the US government.

Way Forward

- **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.

Drishti Input

"Discuss how data deprivation is a challenge to tackle cyber crimes. Also comment whether data localisation will help in solving cyber crimes in India."