Sleepy Classes
Free. Regular. Quality.

MAD- 2020
Day – 43
SECURITY

To Watch the Video, Click Here:

https://youtu.be/-rl3S79IUd4

Question:

What do you understand by Data localization? Do you think blocking off 59 widely used apps linked to Chinese companies will address the same? Critically analyses.

Answer:

- Data localization in the Indian context simply means that companies collecting critical data about consumers must store and process such data within the Indian borders. Prior to the Reserve Bank of India's (RBI) announcement, most data from India was not stored within the country. It was usually stored on a cloud database outside India. The call to localize sensitive data by the RBI convinced many companies like tech majors like Paytm, WhatsApp and Google to change their data storage locations to India by 15th October, 2019.
- Localization mandates that companies collecting critical data about consumers must store and process them within the borders of the country.
- A recent Brookings report on the importance of cross-border data flows discusses five reasons why governments want to localize data:
    - Protection of personal data;
    - Access to data by law enforcement;
    - Ensuring national security;
    - Advancing local economic competitiveness; and
    - Levelling the regulatory playing field

Blocking off 59 widely used apps linked to Chinese companies:

- As specified by the Ministry of Electronics and Information Technology (MeitY), the 59 apps have been banned by the ministry using its power under Section 69A of the Information Technology Act 2000.
- Section 69A of the IT Act says that the central government can ensure that public access to any information (whether an app or a website) is blocked, if it is satisfied that this is necessary or expedient to do so in the interest of the sovereignty and integrity of India, defense of India, security of the State... or public order".
- The government has specifically stated that the misuse of data collected by the 59 apps in question "is a matter of very deep and immediate concern which requires emergency measures.
- The extensive data collection by technology companies, has allowed them to process and monetize Indian users' data outside the country. Therefore, to curtail the perils of unregulated and arbitrary use of personal data, data localization is necessary. This step of banning is the first step in the right direction. Digital technologies like machine learning (ML), artificial intelligence (AI) and Internet of Things (IoT) can generate tremendous value out of various data. It can turn disastrous if not contained within certain boundaries.
- With the advent of cloud computing, Indian users' data is outside the country's boundaries, leading to a conflict of jurisdiction in case of any dispute.
- Also, data is a sovereign right, and every country has a right to protect its citizens' sensitive data.

Indian fintech'sS support data localization because they view data as a vital asset that should be kept within Indian borders. It will ensure a level playing field for the Indian startup ecosystem with respect to global tech giants.

- It is an opportunity for Indian technology companies to evolve an outlook from services to products. International companies will also be looking at the Indian market, and this will benefit the growth of the local ecosystem.

Concerns:

- Also banning the apps without giving the chance of hearing to companies is a **violation of natural justice and** can deter other companies to further invest in India. Apps like TikTok has claimed that it continues to comply with all data privacy and security requirements under Indian law and has not shared any information of our users in India with any foreign government, including the Chinese Government
- The government should have specified what information and evidence the government has indicated as 'misuse' and 'stealing' of data by the apps in question.
- **Technical and financial capacity of global cloud providers** is more important to data security than whether data is stored locally.
- Restricting data flows to try to protect domestic companies from digital competitors can **trigger other countries to retaliate,** harming other local companies that seek to use data to conduct business globally.
- **India will lose policy credibility-** It has also been suggested that India should renege on existing contracts with China. This can be detrimental to India's effort to attract foreign investment. As one of the first things, an investor — especially foreign — tracks is the policy credibility and certainty. If policies can be changed overnight or if the government itself reneges on contracts, the investor will either not investor demand higher returns for the increased risk.

Way Forward:

- Laws like Personal Data Protection (PDP) Bill, 2019 should be passed and enforced immediately. This law is a comprehensive piece of legislation that seeks to give individuals greater control over how their personal data is collected, stored and used.
- Once passed, the law promises a huge improvement on current Indian privacy law, which is both inadequate and improperly enforced. It also includes removal of restrictions on the transfer and storage of personal data outside of India. However, the restrictions on both "sensitive" and "critical" personal data from the initial draft of the bill remain.
- Ideally, like Brookings report shared some good examples of frameworks that allow countries with different approaches to data protection to agree to sets of principles by which cross-border data transfers can occur, should be followed. This kind of collaboration around data is in the early stages, but it is precisely what we need to see more of for the true potential of data to be seized.