RBI's Stance on Data Localisation Rules

Why in news?

\n\n

The government and the RBI are firm on the October 15 deadline for compliance on data localisation standards.

\n\n

What was RBI's order on data storage?

\n\n

\n
- Data localisation is storing of data on a device physically present within the borders of the country where the data was generated.
\n
- RBI, in April, 2018, gave 6 months time to global payment companies to store transaction data of Indian customers within India.
\n
- The data should include the full end-to-end transaction details, information collected/carried/processed as part of the message/payment instruction.
\n
- The requirements apply as those mentioned in the draft data protection bill and draft national e-commerce policy framework.
\n

\n\n

What was the demand?

\n\n

\n
- Global financial technology companies have reportedly sought an extension to the October 15 timeline, with demands to adopt a soft stance on data localisation.
\n
- But the RBI and the government did not favour any extension of the deadline.
\n
- The government has also ruled out data mirroring as an option.
\n

- Foreign payment companies had asked the RBI to allow data mirroring which would allow them to store a copy of the data overseas as well.
  \n

\n\n

Why is it being opposed?

\n\n

\n
- Any move to restrict all cross-border data flows could be counterproductive, on becoming a trade barrier.
  \n
- The norms could have negative impacts on the ability of companies to do business in India.
  \n
- Especially, the U.S. warned that India's policy on the issue will adversely affect American businesses in the country.
  \n
- It may undermine India's own economic goals and may not likely improve the security of Indian citizens' data.
  \n
- It could also break up the Internet if every country in the world insists on keeping data within its territory.
  \n

\n\n

What is RBI's rationale?

\n\n

\n
- The move was to ensure better monitoring of payment service operators.
  \n
- Data localisation would offer supervisory access to data stored with these system providers.
  \n
- It also gives access to data stored by their service providers/ intermediaries/third party vendors and other entities in the payment ecosystem.
  \n
- National security and data sovereignty are other reasons for data localisation rules.
  \n
- As, it is possible that data could be indicted if it is stored on American servers and India faced US sanctions.

\n

\n\n

What are the limitations to data localisation?

\n\n

\n
- **Global players** like banks, e-commerce majors, fin-tech service providers and credit card companies prefer to store and process data at one or two global centres.
\n
- So moving processes implies higher costs and disruption for them.
\n
- New teams must be hired and trained, and security procedures have to be reviewed and modified.
\n
- **Local infrastructure** in India suffers from severe deficiencies.
\n
- Indian data-transmission speeds are slow by global standards.
\n
- Server capacity is low and costs are high, and likely to rise as demand is artificially boosted.
\n
- So RBI's insistence may lead to a situation where smaller payment companies stop offering services in India.
\n
- It will also impose higher costs on the start-up ecosystem since any Indian start-up will pay higher costs to include payment options.
\n

\n\n

\n
- **Legal** - The Srikrishna Committee recommendations on data protection are now only open for public feedback.
\n
- So as of now, India neither has a functioning data protection law nor adequate security standards in practice.
\n
- Evidently, there have been instances of massive leaks and hacks of sensitive information, including payment records.
\n
- **Surveillance** - Law and order departments and security agencies currently operate in a legal vacuum, making surveillance another grey area.
\n

- They can search and survey all sorts of digital data without any checks or balances.
  \n
- Indeed, there is evidence that foreign intelligence agencies also collect a massive amount of Indian data and meta-data.
  \n

\n\n

How is it elsewhere?

\n\n

  \n
- Data localisation is not a new concept but has picked up pace after 2013.
  \n
- It is when America's National Security Agency contractor Edward Snowden leaked classified documents.
  \n
- It showed how the US government had accessed data to conduct surveillance on foreign allies.
  \n
- Since then, countries like Germany have taken steps to ensure that sensitive data stay within their borders.
  \n
- Many other countries like Russia and China have very stringent laws around data localisation.
  \n
- It is largely driven by the fear of losing critical data to hackers and spy networks of rival countries, as well as systemic risks during times of conflict.
  \n

\n\n

What lies ahead?

\n\n

  \n
- **RBI's** firm stance on sticking to the deadline is a welcome move.
  \n
- It should now send a stronger signal by imposing stiff penalties for non-compliance.
  \n
- **Sectors** - However, India should be careful in imposing data localisation across all sectors.
  \n
- Adopting data localisation in few sensitive sectors like financial services and

relaxing on e-commerce and cloud computing is valid.
\n
- E.g. in Australia and Canada, data localisation rules are applied only to specific sectors like healthcare, telecom and finance
\n
- **Law** - Data localisation rules must be backed up by a strong data protection law to clearly define and limit surveillance powers.
\n
- Policy measures to encourage the creation of higher server capacity and enabling cheaper and faster data transmission are essential.
\n
- **Multinational companies**, on their part, should take a more proactive role in following local rules.
\n

\n\n

\n\n

Source: Economic Times, BusinessLine, Business Standard

\n