Data Localisation and India's stand

June 20, 2019
Manifest Pedagogy

In the era where data is the new oil, the data localization has taken centre stage. India's draft e-commerce policy and B N Srikrishna committee report is of prime importance for an aspirant. The pros and cons of data localization for the hugely populated country like India has to be studied in detail as we can expect an essay on the same.

In news

US's recent criticism on India's data localisation norms and draft e-commerce policy.

Placing it in syllabus

Internal Security

Static dimensions:

- What is Data localisation?
- **India's rules in place for data protection**
- Justice Sri Krishna committee report on data protection

Current dimensions:

- Draft e-commerce policy 2019
- Importance of Data localisation

Content

Recently **U.S. criticised India's proposed norms on data localisation as 'most discriminatory'** and **'trade distorting'** in its Trade Representative's 2019 **National Trade Estimate Report on Foreign Trade Barriers.** It said that number of data

localisation requirements would serve as significant barriers to digital trade between the US and India.

In July 2018, the Indian government published a **draft Personal Data Protection Bill**. The report has also noted that if passed into law, the bill would impose onerous burdens on firms, especially foreign firms, that process personal information.

What is data localisation?

Data localisation is the **act of storing data on any device physically present within the borders of a country**. As of now, most of these data are stored in a cloud, outside India.

Localisation mandates that companies collecting critical data about consumers must store and process them within the borders of the country. The RBI had issued a circular mandating that payments-related data collected by payments providers must be stored only in India, setting an October 15, 2018 deadline for compliance. This covered not only card payment services by Visa and MasterCard but also of companies such as Paytm, WhatsApp and Google which offer electronic or digital payment services. RBI's diktat has followed the draft data protection law recommended by Srikrishna committee in 2018.

Importance of 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. 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.
- **For 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 too.
- **According to Justice Srikrishna Committee report**, **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.
- Technology playfields are not even. A developing country such as India may be playing catch-up with a developed nation, which may be willing to
- offer liberal laws. It may not be wise for India to have the liberal rules as other nations would.

India's rules in place for data protection

- Currently, the only mandatory rule on data localisation in India is by the **Reserve Bank of India for payment systems.**
- The second piece is the **Draft Personal Data Protection Bill, 2018** itself which has specific requirements on cross-border data transfers.
- 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.

Why are companies reluctant to comply?

- The disadvantage for a company compelled to localise data is obvious – costs, in the form of servers, the UPS, generators, cooling costs, building and personnel. Companies feel that infrastructure in India is not yet

ready to support this kind of ecosystem.

- 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.
- Observers feel it is still not comparable to the EU General Data Protection Regulation (GDPR), which took a few years to draft, adding scholarly and academic depth to the consultations, inputs and the final wording of the law.
- Above all, localisation might save Indian data from foreign threats but placing the servers on home soil increases the risk of domestic threats while also dealing with the challenge of inadequate infrastructure.

Status of Data localisation in other countries

- **Australia and Canada: they protect their health data very carefully**

- **Vietnam:** It mandates one copy of data to be stored locally and for any company that collects user data to have a local office, unlike the EU's GDPR; citing national interests.
- **China** mandates strict data localisation in servers within its borders. International reports refer to data protection laws in Vietnam and China as being similar, in that they were made not so much to protect individual rights as to allow government to control data.
- **For the EU,** it is clear that customer is 'king'. Their GDPR is agnostic to technology and sector.
- Interestingly, **the U.S.** has no single data protection law at the Federal level. It does, however, have individual laws such as the HIPAA (Health Insurance

Portability and Accountability Act of 1996) for health care, another for payments, and the like.

- **Brazil, Japan, Korea and New Zealand** have put in place data protection laws.
- **Chile** has recently announced the setting up of an independent data protection authority, while Argentina is currently reforming its privacy legislation.

Key highlights of B N Srikrishna Committee report on data protection

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India.
- Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India.
- The law will not have retrospective application and it will come into force in a structured and phased manner.
- The Aadhaar Act needs to be amended to bolster data protection.
- An independent regulatory body called Data Protection Authority(DPA) will be responsible for the enforcement and effective implementation of the law.
- The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA.
- Penalties may be imposed for violations of the data protection law.
- The state can process data without consent of the user on ground of public welfare, law and order, emergency

situations where the individual is incapable of providing consent, employment, and Reasonable purpose.
- The law will cover the processing of personal data by both public and private entities.
- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.
- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses.

Draft e-commerce policy 2019

The **Department of Industry and Internal Trade** has released the draft National e-commerce Policy that sends a clear message that India and its citizens have a sovereign right to their data.

- **Issues addressed**:

1. Data
2. Infrastructure development
3. E-Commerce marketplaces
4. Regulatory issues
5. Stimulating domestic digital economy
6. Export promotion

- Govt to be given access to source code, algorithms of AI systems, Impose customs duties on electronic transmissions to reduce revenue loss.
- Bar sharing of sensitive data of Indian users with third party entities, even with consent.
- All e-commerce websites, apps available for downloading in India to have a registered business entity here.

- Location of the computing facilities like data centres, server farms within India.
- Firms to get 3 years to comply with local data storage requirements.
- Data storage facilities to get ‘infrastructure status’.
- FDI in e-commerce only in marketplace model.
- Integrating Customs, RBI and India Post to improve tacking of imports through e-commerce.
- E-commerce startups may get ‘infant industry’ status.
- No separate regulator for e-commerce sector.
- E-consumer courts to be developed.

Cons of e-commerce policy

It does not have parameters for its implementation. The **government has termed data as a ‘National Asset’** and businesses collecting or processing sensitive data in India which is stored abroad will not be allowed to share it with other businesses outside the country, third parties or foreign governments without prior permission. While the implications of such a law could have widespread effects on the way tech giants such as Google, Facebook,, the proposed policy does not explain how the government plans to implement these changes.

While the **draft policy does mention how a handful of companies dominate the digital economy capitalising on the data** they have gathered ,it fails to talk about how that advantage is being amplified by the use of new technologies such as Artificial Intelligence and Machine Learning today.

Way ahead

- The importance of the ability to share data is as important as the existence of data itself. Cross-border data flows are and will remain instrumental in shaping the future of the world.
- A mirror site overseas would help detect frauds and spot money laundering patterns because they often take place

across borders. But ranging from rising strategic concerns from threats such as foreign surveillance, to economic aspects like domestic protectionism, data localisation is viewed as a solution or at least part of it.

- Evaluating both pros and cons of data protection, it is very much needed to take certain measures for storage and the future of India via-a-vis trans border data flows.
- To enable better law enforcement, it is essential to reform the Mutual Legal Assistance Treaties (MLATs) by granting certainty to practices and procedures while minimising discretion.
- Enter into Global Privacy Frameworks and Data Sharing Agreements to ensure criminals are appropriately brought to justice while protecting an individual's right to privacy and promoting GDP growth.
- The way forward would be to signing a data sharing agreement under the Cloud Act, 2018 with the US and also seeking to work with EU after qualifying the adequacy requirements.
- Legal security of data stored in India a due-process of law for access to data. The following factors must be adhered to before data is accessed by the state for law enforcement and investigation purposes:

1. An inclusive definition of the phrase 'Security of State.'
2. The entities/bodies which are authorised to process personal data.
3. An inclusive list of situations demanding processing of personal data.
4. A safety-net regulatory mechanism to approve processing of personal data (ring-fenced from political or economic influence).
5. Disaster Management & Recovery – prescribing the specifications for recovering & damage control in the

event of a breach

- Setting security standards for data centres and allowing them to host data if said standards are met.