Data Localization in India – Pros and Cons.

Dinesh Agrawal
Symbiosis Institute of Business Management, Pune, India.
Dinesh.agrawal06@gmail.com
Ph.No: +919769855712

Abstract -In the era where "data is the new oil", the data localization has taken center stage. Data localization is a measure adopted to give countries increased control over the data belonging to their citizens and residents. Due to the transient and pervasive nature of data on the internet, its security is constantly threatened and indeed been breached at several instances. Data localization is therefore conceived as means of enforcing data protection regime to secure data of the citizens and the critical interests of the nation state.

Many governments insist that data localization is the only way forward to ensure that the data on the internet is safe and secure. China, Russia, Australia, Canada, European Union and several other countries have already adopted data localization provisions.

The Indian government is also in favor of adopting the data localization. On July 2018, the Indian government published a draft Personal on Data Protection Bill. This bill will imposes troublesome on firms that process personal information.

The research aims to study what data localization means and its pros and cons from Indian perspective.

Index Terms — Data Localization, Data Protection, Data Security, Data Safety. Data Privacy

INTRODUCTION:

Data is any collection of information that that can be easily accessible and read by computers. People information like their messages, social media posts, online transactions, and browser searches is considered as data. Big data refers to the immense amount of data that can now be collected, stored, and analyzed to find patterns. This large collection of information about people's online habits has become an important source of profits. Individual's online activity can expose a lot about individual and companies find it valuable to use the information to target advertisements to individuals. Governments have also gained interest in these data sets for policymaking.

What Is Data Localization?

- Data localization is the means of storing data on any device that is within the local data center (present within the borders) of the specific country where the citizen's data is generated.
- Localization mandates collecting companies to store and process critical consumer data within the borders of the country.

India in favor of Data Localization

In early April, the RBI issued a circular mandating that payment data be stored only in India by October 15. This covered every global payments & technology companies and various domestic & foreign prepaid payment instruments (PPIs). As per the clarification issued by RBI on overseas processing of strictly domestic transactions, The processing can be done abroad, however the data need to be brought back to India within one business day or 24 hours from payment processing and deleted from the systems abroad, whichever is earlier. The final data should be stored in India only.

The draft copy of Personal Data Protection Bill, 2018 reported by the Committee of Experts under the chairmanship of Justice B. N. Srikrishna also given an emphasis on data localization. The report states that, every data fiduciary is required to store one serving copy of the personal data on a server or data center that is located within the territory of India. The data fiduciaries are likely to find this obligation onerous, as it will increase operational costs for most of them. This restriction may also operate as a trade barrier and hinder the ability of global companies to transfer and process personal data across different jurisdictions. The Bill states that critical personal data shall be only processed in a server or data center located in India. This effectively means that such data cannot be transferred to any country outside India. It may be a challenge for businesses to service Indian consumers solely through the data centers in India.

The regulations mentioned in Personal data protection Bill is expected to affect Tech companies like Mastercard, Visa, Paypal, American Express, Amazon, Facebook, Microsoft etc. They will be forced to store data in local data center.

LITERATURE REVIEW:

(Guo, 2016)Edward Snowden's 2013 revelations regarding the U.S. government's secret surveillance program by National Security Agency on surveilling online information of both American and foreign citizens and companies triggered other governments realize the potential of utilizing the internet as a means to collect, analyze, and

store data and to come up with data localization laws to protect the data with their territory.

(Anupam Chander, 2015) Chander and Le define localization to include all measures that "encumber the transfer of data" across national borders. Such measures can take a variety of forms, like preventing information from being sent outside the country; requirement to obtain individual consent before making the transfer; storage of a local copy of the data; and imposing taxes on data exports.

Russia

(Kulikova, Jan. 17, 2014) Following the NSA revelations in the summer of 2013, Sergei Zheleznyak, a deputy speaker of the lower house of the Russian parliament and a member of the Committee on Information Policy and Information Technology and Communications, called on Russia to strengthen its "digital sovereignty" through "legislation requiring e-mail and social networking companies [to] retain the data of Russian clients on servers inside Russia, where they would be subject to domestic law enforcement search warrants." In spring 2013, the Minsvyazi (Russian Ministry of Communications) drafted an order forcing telecommunications and Internet providers "to install equipment allowing data collection and retention on their servers for a minimum of 12 hours." This obligation is directed for websites and Internet service providers that carry data between users and computer servers. Data localization requirement is met by asking Russian Internet service providers to save data locally. This order gives the Russian Federal Security Service (FSB) "direct access to a wider range of data than was possible before—including users' phone numbers, account details on popular domestic and overseas online resources (like Gmail, Yandex, Mail.ru etc [sic]), IP addresses and location data—without a court order, for the purposes of national anti-terrorist investigations."

European Union

(Union, 2016)Passed in May 2016, the European Union (EU) General Data Protection Regulation (GDPR) replaces the minimum standards of the Data Protection Directive, a 21-year-old system that allowed the 28 EU member states to set their own data privacy and security rules relating to the information of EU subjects. Under the earlier directive, the force and power of the laws varied across the continent.

China

(Xia, 2018)China's Cyber security law took effect in 2017 and it requires critical information infrastructure operators (CIIOs) to store personal information, important data collected and generated within the territory. The network operator classification depends on its industry and on how much a data breach would harm the public interest. Network operators in industries like public communication and information service providers, energy, finance, and public services are more likely to be considered CIIOs.

Under GDPR, organizations are subject to new, uniform data protection requirements—or could potentially face hefty fines. GDPR is a game-changer to organizations worldwide. At minimum, the regulation demands:

- Data protection accountability. Companies must demonstrate that considerable security measures are in place to protect users' private data. The ante is upped for companies delving in high-risk areas.
- Data subjects' right to access, rectification, erasure and portability. Organizations need to validate the individual's identity, swiftly produce personal data it processes, and correct, erase or transfer data on request.
- Data breach notification. A personal data breach "leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" must be reported within 72 hours of discovery

Canada

(Adam Kardash, 2017)Businesses that engage in the collection, use, disclosure and management of personal information in Canada need to be cognizant of the regulatory framework governing the privacy landscape in order to stay compliant. The data protection regime in Canada is governed by the following four private sector privacy statutes:

1. the Federal Personal Information Protection and Electronic Documents Act (PIPEDA);
2. Alberta's Personal Information Protection Act;
3. British Columbia's Personal Information Protection Act; and
4. Québec's An Act Respecting the Protection of Personal Information in the Private Sector (collectively, Canadian Privacy Statutes).

PIPEDA governs the inter-provincial and international collection, use and disclosure of personal information. It also applies to organizations that collect, use and disclose personal information during a commercial activity that takes place within a province. In addition to these four statutes, Canada has also enacted anti-spam legislation (CASL).

Findings (based on literature review):

Thus from Literature review we can see that Data localization is gaining momentum and Companies that fall within the scope of data localization laws will need to invest in building local infrastructure to comply with these regulations. Businesses will have to carefully decide on there operations in these increasingly restricted markets.

RESEARCH FINDINGS:

On conducting secondary data analysis and personal interviews with executive from Fintech Company below are Pros and Cons for Data localization.

PROS:

Protectionism: Governments want to give a competitive edge to their local corporations (e.g. Reliance/PayTm companies welcomed this decision). The flow of data to external countries will be restricted, hence the data will be available for internal use by local companies. This will create an information asymmetry which will turn out to be favorable for the local companies.

Taxation: Advocates of Data localization consider Data as national resource. This means that the government of the nation should have a right on the revenue generated from that resource. Just like the inflow and outflow of goods and services are taxed, the movement of data in and out of the nation should also be taxed. These additional taxes can then be used by the government for more social programs.

Foreign Surveillance: Secures citizen's data and provides data privacy and data sovereignty from foreign surveillance. Example - Facebook shared user data with Cambridge Analytica to influence voting.

Enforcement by local law agencies: Unfettered supervisory access to data will help Indian law enforcement ensure better monitoring. It gives local governments and regulators the jurisdiction to call for the data whenever required. Minimizes conflict of jurisdiction due to cross border data sharing and delay in justice delivery in case of data breach.

Building an Digital Ecosystem: Higher foreign direct investment in digital infrastructure will boost Indian Economy. Data center industries are expected to benefit due to the data localization which will further create employment in India. Creation of digital industry and digital infrastructure will help in development of AI based applications.

CONS:

Infrastructure: Infrastructure in India for efficient data collection and management is lacking. It is a big challenge to develop efficient infrastructure at a faster pace.

Investment: Organizations will need to increase investment in the construction and maintenance of their own local IT infrastructure.

Safety of the data: Without efficient infrastructure, the data is prone to cyber-attacks. And the risk is severe here because it is financial data.

Security Risks: Locating data within a given jurisdiction does not in make data secure. It is prone for hacking and security breach and requires law for data controllers to strictly protect the data that they're entrusted with.

Cost: Storing data in India means higher operational costs for payment system operators. For cross-border transactions, they have to store the data in two places, which increases costs. There is a probability that these extra costs may pass on to the consumers. Also there is no guarantee that they will delete the data elsewhere. They may continue to store and analyze the data for their own advantage.

Global Trade: Data localization is a threat to the free flow of data. US is against to the data localization laws. Its stance is natural because it increases the operational costs of US companies. India-US bilateral relations are important for both countries because we are intertwined in export and import of IT services, professionals and goods etc. So, imposing data localization laws without threatening the Indo-US relations is another challenge.

Innovation: Data localization laws may threaten the innovation attempts in the digital payments industry as company will bear additional financial burden and may restrict fund in Research and Development.

Government Surveillance: Data localization may result in government surveillance of its citizens. It is also against intellectual property rights because they use their intelligence to form systems that can benefit from the data it generates, but in the end, they are deprived of these benefits and someone else may use this data in their favor.

CONCLUSION:

Data localization is relatively a new concept. Taking steps towards ensuring the privacy and security of the citizens' data is a very progressive step. In the starting, companies may face technical difficulties and will bear additional costs to run the business. However, we will come to know the real consequences over the period of time.

REFERENCE:

1. Anupam Chander, Uyen P. Le, Data Nationalism , Emory Law Journal, Vol. 64, No. 3, 2015
2. Alexandra Kulikova, Data Collection and Retention in Russia: Going Beyond the Privacy and Security Debate, GLOBAL PARTNERS DIGITAL (Jan. 17, 2014), http://www.gp-digital.org/gpd-update/data-collectionand-retention-in-russia/
3. Adam Kardash, Brandon Kerstens, The International Comparative Legal Guide to:Data Protection 2017, 4th Edition https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Canada-2017.pdf
4. https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html
5. "Regulation (EU) 2016/679 of the European Parliament and of the Council," April 27, 2016

6. https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?noredirect=on
7. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244
8. https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574
9. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
10. http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications
11. https://www.ibm.com/downloads/cas/OANPKWGY
12. Dhont, Jan and Woodcock, Katherine (2015). "Data localization requirements: Growing trends and impact for company compliance," Corporate and Ethics Professional. http:// www.lorenz- law.com/wp-content/uploads/Data-localization-requirements-Growing-trends-and-impact-of-compnay-compliance1.pdf