International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Localisation and itsImpact on Indian Economy

Swastik Rastogi[1], Mayank Singh[1], Rinku Raheja[1]

[1]Student, Department of Computer Application, National P.G. College Lucknow.
[2]Assistant Professor, Department of Computer Application, National P.G. College Lucknow.

ABSTRACT

Data Localisation initiatives are being taken by the government are pernicious for the economy of the country. This research would give a review of data localisation policies prevailing in Indiaand what further attempts are being made by the Indian government to protect users' privacyas well as to ensure National Security. This research concludes that efforts to maintain national security are great, althoughthese efforts are not in favour of the economy. However, accessibility over citizen's data would give law enforcement agencies a power to maintain the rule of law.At this time, it is essential to develop policy initiatives both to ensure transparent and clear norms on data security, also as to enable higher levels of digital innovation in our country.

Keywords— National Security, PDP Bill, Data Centre, Data Localisation

Introduction

The dream or insight of an internet network without any border that works as an open-source accessible to everyone is slowly retreating to space is being political and getting rendered due to economic, cultural, and geopolitical differences and imbalance. Many nations are taking a variety of measures for establishing their absolute or total control over data within the country's national boundaries is, which is called 'data localisation'.

The term 'data localisation' generally refers to storing the data physically within a country's national boundaries, albeit sometimes it is more widely relates to the restrictions or limitations implied on the flow of data across the country's border. Therefore, on this approach, Chander and Le in 2015 defined localisation, which included all the measures that *"encumber the transfer of data"* (i.e., determining the obstructions faced during the transfer or flow of data) across national borders. Some of the measures they listed include – restraining information or data from being sent outside the country, obtaining an individual's consent before making the transfer of data, storing a local copy of the data physically within the country, and imposing taxes on the export of data. Taking a step further, Selby in 2017 suggested that the "localised data routing" must be imposed, which means that the data packets which are exchanged between domestic users on Internet services must flow through internal networks only. This can also be seen as another category of data localisation.

Data Localisation in India

The Indian government is taking severe steps to localise the data of the country within its boundary to secure citizen's data, data privacy, data sovereignty, national security, and to ensure economic development of the country. The Indian government has forged and introduced 'multiple policy instruments' over the past few years, which enlisted that only specific types of data and information must be uploaded on those servers only, which are located physically within India's national boundary. These localisation manoeuvres and related schemes have given rise to nocuous debate among corporations, foreign stakeholders, civil society actors, politicians, business alliances & guilds, and governments.

The Indian government, on many occasions, has asked the USA Government to serve summonses upon Google as well as upon Facebook, Twitter, and others for failing to prevent the dissemination of speech prohibited under Indian Law. However, those requests were rejected due to considerations about US civil liberties.

Recently in Union Budget 2020 Indian Government launched an incentive policy for the non-public sector firms to build data centre parks in India which is able to create a cheap environment to store knowledge regionally. However, the industry would require not merely SOP if the government needs to attract non-public firms to set up data centres parks within the country. The businesses and firms will also need support in terms of land and property, 24*7 internet connectivity, uninterrupted power and much more.

Personal Data Protection Bill & RBI's Policy

In August 2017, the Ministry of Electronics and Information Technology had constituted a committee of experts, Chaired by the Retired former judge of the Supreme Court, Justice BN Srikrishna. The Committee task given to the committee was to examining issues related to data protection in India and formulating a draft data protection statute. In July 2018, the Committee released its Report, as well as the proposed PDP(Personal Data Protection

Bill), 2018. The draft bill says that sensitive personal data can be processed only with the explicit consent of the person. Further, the consent needs to be informed, clear, and specific, as defined by the bill. It states that sensitive personal data which include passwords, financial and health data, sexual orientation biometric data, and other religious or political belief. The draft Bill also has a provision where the person "shall have the right to restrict or prevent continuing disclosure of personal data". There is a provision for the Centre to notify categories of data as critical, which will only be processed in servers located in India. Personal data have to be stored in India, but can be handled outside with the consent of the person. It also notifies penalties for not following its provisions.

Starting with Reserve Bank of India, the Indian government had also issued a directive in April 2018 on 'Storage of Payment System Data'. It had advised all payment system providers to ensure that within six months, the entire data relating to transactions and payment systems operated by them should be stored in a system only in India. Later in June 2019, the Reserve Bank said that all the data related to payments must be stored only in India, and data processed abroad should be brought back to the country within 24 hours. Currently, India has four sectoral policies that are based on data localisation its requirements. They are based on type of data, for sectors including banking, telecom, and health - these policies include the RBI Notification on 'Storage of Payment System Data', the FDI Policy 2017, the Unified Access License, and the Companies Act, 2013 and its Rules, The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, and the National M2M Roadmap.

The following table shows the Indian Laws and policies enabling data localisation:

Category of Data	**Policy/Law**	**Cross-Border Flow of Data**
Critical Data	Personal Data Protection Bill, 2018	No Cross-Border Flow of Data Permitted
Personal Data		Cross-Border Flow of Data Permitted as long as copy maintained in India
Personal Data not collected in India		No Restriction on the flow of Data
Public IoT Data	e-Commerce Policy	Cross-Border Flow of Data Permitted as long as copy maintained in India.
E-Commerce Data		
Payment Systems Data	RBI Circular	No Cross-Border Flow of Data Permitted
e-Pharmacy Data*	e-Pharmacy Regulations	
Subscriber and User Data	Unified Access License for Telecom	
Subscribers' Databases (BroadcastingSector)	FDI Policy	
Companies' Account related Data	Companies (Accounts) Rules,2014	Cross-Border Flow of Data Permitted as long as copy maintained in India
Insurance Policy Holder Data	IRDAI Regulations	
Government Data	Guidelines on Contractual Terms Related to Cloud Service	

The Economic Perspective

The development, widening of the Internet network, and accompanying flow of data have been a critical factor for the growth of the economy in the past few decades. It seems to be an increase in demands of data localisation in various countries, however, ignoring the fact that one of the boons of the Internet network has been to create efficient distribution of data and services globally. In 2014, students of Mckinsey Global Institute did a survey and found that the direct impact of cross-border data flows had raised world GDP by 3% (worth about $2.2 trillion in 2014), which exceeded the contribution of trade in traditional goods in that year (Manyika et al., 2016).

However, the 'data' or information, also known as "the new oil," is significantly controlled over by some handful of corporations like that Google, Amazon, Apple, Facebook, and Microsoft as per The Economist in 2017. As per the survey, in terms of hosting locations, 42% of the world's top million sites are based in the United States and Canada, at second number it comes to Europe with a mark or 31% and only 12% in the Asia Pacific region and the remaining in other parts of the world (Manyika et al., 2016). Therefore, the measures are being adopted by various nations to bridge these gaps that range from a push for tighter regulation of the technology sector to looking at data localisation as a tool to promote the domestic industry. India's new policy of 'push towards localisation' also refers to the objectives like "nurturing digital innovation" and "stimulating domestic digital economy" (e-Commerce Task Force, 2018). Similarly, the report by Srikrishna Committee's broached to the "positive impact of server localisation on the creation of digital infrastructure and digital industry".

While examining the effects of data localisation measures on the economy, one must also keep in mind that what impact it would have on an individual's business. An Indian citizen can practice any profession or can carry on any occupation, trade, or business as per Article 19(1)(g) of the Indian Constitution. However, Article 19(6) enumerates the nature of restrictions that can be imposed by the state upon the above rights of the citizen. Constraints in this regard may be imposed based on activity against being antisocial or against public welfare, etc. Notably, the government can impose licensing and other restrictions on businesses. Accordingly, in the interests of public welfare, the state may legitimately impose restrictions on or can ultimately ban the cross-border flows of data despite the fact that what apparent effect it may have on businesses and its outcomes. However, it may be difficult to demonstrate that localisation measures will result in a violation of the rights under Article 19 (1) (g), the effects of localisation on businesses should still be a consideration from a policy point of view. The growing yet intertwined nature of the economy with the Internet implies that there will necessarily be many economic implications to curb online businesses.

Measuring the Economic Impact

One of the major arguments against mandatory localisation stems from the cost that it is likely to impose on businesses and, consequently, their consumers and the economy as a whole. Comprehensive data localisation policies will mean that businesses and other users – both domestic and foreign – will no longer have the flexibility to choose the most cost-effective or task-specific location to store their data. These efficiency losses will ultimately be passed onto the public in the form of higher costs of service. While the literature on data localisation frequently makes these assertions, only a handful of studies have attempted to undertake an actual cost benefit analysis of data localisation measures.

Costs of Data Localisation

Despite the lack of significant economic literature on this subject, the purported costs of localisation measures are often raised as a ground to argue against the imposition of such measures. Most commentators refer to just two prominent studies on this subject – a 2014 study by the European Centre for International Political Economy and another one in 2015 by Leviathan Research (in association with Google) – both of which note that the costs of localisation outweigh its benefits. While the findings of these studies remain contested (Gurumurthy & Chami, 2017), in the absence of any other evidence on this subject, we find it useful to examine the findings of these reports in some detail. In the study conducted for the European Centre for International Political Economy, Bauer et al. (2014) quantify the expected losses from data localisation requirements and related measures in seven jurisdictions, including India. They find that imposing economy-wide data localisation requirements could reduce the Indian GDP by 0.8% and domestic investments by 1.4%.The study also looked at the welfare costs of data regulation on a per-worker basis and find that for India, the loss per worker would be equivalent to 11% of the average monthly salary. The authors finally state that "any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy". Building further on this study, Bauer et al. (2016) found that the effects of data localisation on specific sectors vary depending on the extent to which a particular sector is dependent on data inputs. As a result, the negative impact was found to be higher for sectors like communication services, financial services, and other data-intensive businesses. This led the authors to conclude that tighter restrictions of free flow of data would cause an economy's production structure to shift back towards sectors such as agriculture, raw materials, and natural resources. Moving away from the macro-level approach of the above studies, Leviathan (2015) looked at the effect of forced data localisation laws on individual businesses by calculating the cost difference on a per-hour, per-server level. The study focused on public "Infrastructure as a Service" (IaaS) cloud computing providers and found only seven cloud providers globally met the selected criteria. None of the identified providers had data centres in India. As a result, domestic users would either have to use traditional datacentres, with accompanying capital investment in hardware and periodic upgrade costs, or they would have to enter into specifically negotiated business contracts with non-public cloud providers. In the case of countries that did have such data centres, the researchers found that forced data localisation laws would require local companies to pay 30%-60% more for theirs.

Arguments in favour of Data Localisation

National Welfare: Data localisation is necessary to ensure citizens' data, data privacy, data sovereignty, national security, and economic development of the country.

Enforcement by local law agencies: Localising personal data would help law enforcement agencies' efforts to access information to unmask crime and also in gathering evidence for prosecution. If personal data is stored within India, then the possibility of a foreign entity refusing access to such data would be reduced.

Avoiding resultant vulnerabilities of dependence on fibre optic cable network: A large amount of data is transferred from one country to the other through undersea cables. The location of almost every undersea optic fibre cable in the world is publicly accessible, which creates the opportunity of the vulnerability of the internet and cross-border transfer of data.

Preventing foreign surveillance: Data related to critical state interests of the country must be brought up for absolute processing in India, and any such obligations should be limited to it. Thus, it will help in the prevention of foreign surveillance over critical personal data. It should be exclusively processed within the territory of India.

Cost of data protection: All or most legal obligations give rise to economic costs for regulated entities, and thus a mere increase in costs cannot be a reason not to introduce legal change. Instead, the costs incurred due to rules demanding local processing outweigh the benefits of such a requirement.

Building an AI ecosystem: In the future, Artificial Intelligence is expected to become available in all significant aspects of life which are currently affected by technology and will be a substantial driver of economic growth. The creation of the digital industry and digital infrastructure are essential for developments in AI and other emerging technologies. This necessitates data to be exclusively processed or stored in India.

Digital Infrastructure: The server localisation can have a positive impact on the creation of digital infrastructure and the digital industry through enhanced connectivity and the presence of skilled professionals. It will bring higher foreign direct investment in digital infrastructure.

Arguments against Data Localisation

Safety of the data: Restricting service providers to use the infrastructure within a few countries would increase the threats to data security. If all the data is stored within the geographical boundaries, governments will be able to collate all the data and invade the privacy of individuals if needed.

Data versus Data Centre:Only the location of data centres within the physical boundary of a country does not entitle law enforcement agencies to possess better access to data held by such data centres. Access to data rely on who has custody, control, and possession of the actual data - and that may not necessarily be with the entity that provides the local hosting facility.

Data Localization can not stop foreign surveillance: Several foreign governments and their agencies are reported to use sophisticated malware for data surveillance. Thus, physical accessibility to data centres or processing facilities is not technically necessary in order to conduct surveillance activities.

The threat of domestic surveillance: By extension of the same argument as the advocates of data localization, the local government may exercise higher coercive power over domestic businesses storing data to circumvent legal protections.

Cost of Localization: This is the most crucial point of view on data localisation. Policymakers are not entirely agreeing with the substantial costs of reorganizing and relocating data and operating new data centres, which could discourage if not bar investment, especially from small and medium enterprises (SMEs). The Indian public cloud services market is set to more than double to $7 billion by 2022. According to estimates, Enterprise spending on data centre infrastructure software will rise 10% to $3.6 billion in 2018.

Cost of the data breach: According to the reports, the global average cost of a data breach is already up to 6.4% over the previous year to USD 3.86 million, and setting up data centreparks in India would create a honeypot for hackers and crackers.

Reduced quality of services: Data localization could significantly reduce the quality of the services consumers receive since companies extract insights and other useful information to improve their services.

Recommendations

As we have analysed from the surveys (as mentioned above), there are some policies which are responsible for maintaining harmony between various nations or otherwise 'data', which is no less than a 'fuel' can create tensions among nations in no time as directly or indirectly it is affecting the economy. The rich countries (e.g., USA) are becoming more productive and more prosperous day-by-day as they are keeping the data of their member countries too.

Therefore, our recommendation from this analysis will be that India must take a step forward for localizing data within its boundaries. However, we cannot defy to the fact that India does not have a well-developed infrastructure to ensure the security of data and developing one will cost a lot. However, before we quickly conclude, we must not forget that India has the second-largest population in the world. Currently, around millions of petabytes of digital data is being processed in India within a year.Then why to let some other countries get rich on something which is ours? The development of the proper infrastructure will not only help India keeping the data within its boundary, but it will also result in creating new jobs in the IT sector fields. So in this way, we can employ our engineers and technicians who go to other countries.

Also, many implications which are being faced as per the RBI's Personal Data Protection Bill of 2019 will get solved. However, we must keep in mind that challenges like cyberattacks need to get tackled before taking any major step.

Conclusion

Data localization has been a particularly polarizing topic in India over the past six months. In recent years, there is a massive explosion in data

generated by the users in India connected over the internet. In 2010, Digital data was around 40,000 petabytes in India. However, it is more likely to reach up to 2.3 million petabytes by 2020 — twice as fast as the global rate. Therefore, India will become the second-largest investor in the data centre market and the fifth-largest data centre market by 2050 if it houses all of this data.

The report by real estate and infrastructure consultancy Cushman and Wakefield describes that the size of the digital population in India presents a huge potential demand for data centre infrastructure, so setting up data centres parks in India can not be denied very clearly.

Following an assessment of each of these perspectives, we find that the costs of introducing broad and sweeping data localisation norms are likely to outweigh its benefits, from a rights-based perspective as well as an economic one. However, this is not to suggest that data localisation can never qualify as a justified measure. There may indeed be circumstances where local storage (and even processing) of the data can be justified, particularly on specific normative grounds.

There are various reasons for restrictions of cross-border data flows and localisation. These range from privacy protection to national security to industrial policy. Their immediate impact is more substantial compliance burden, higher cost of business operation, and over the medium to long-term, multiplication of redundant data. However, taking steps towards ensuring the privacy and security of the citizens' data is a very progressive step.

References

[1] The Localisation Gambit https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

[2] Why data localisation triggers heated debate - TFIPOST. https://tfipost.com/ians-news/why-data-localisation-triggers-heated-debate/

[3] Storage of Payment System Data https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[4] Union Cabinet approves introduction of Personal Data Protection Bill in Parliament-The Hindu https://www.thehindu.com/business/union-cabinet-approves-introduction-of-personal-data-protection-bill-in-parliament/article30169881.ece

[5] Unpacking policy moves for sovereign control of data in .... https://cyberbrics.info/unpacking-policy-moves-for-sovereign-control-of-data-in-india/

[6] Telecom Regulatory Authority of India Policy Issues https://main.trai.gov.in/sites/default/files/rec22july.pdf