Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Data Localization

Jigyasa Singh[a]

[a]Lloyd Law College, Greater Noida, India

Received 08 December 2022; *Accepted* 12 December 2022; *Published* 20 December 2022

In this digital era, where there is an immense threat to the privacy of the data of individuals, data localization is a great approach one can opt for. To protect the energy that is highly consumed by the data servers outside India, we should be taking steps to store the data locally, so that renewable energy can boost up. Data localization is not a one-day story, it's a collective effort with great expertise from Data Collection to processing of the Data. Law enforcement agency easily tracks local data. Many legal acts and bills have been passed for ensuring the privacy of individuals which comes under the broad concept of data localization. Countries across the globe are practising such methodology to prevent cyber espionage and for the growth of their respective economies. Therefore, it is of utmost importance that we should be looking for the establishment of a Data centre locally.

Keywords: *territorial jurisdiction, data localization, renewable energy, cyber espionage.*

INTRODUCTION

Data is a set of information that is being translated into a form that is efficient for movement or processing. Data can be in the form of texts, figures, images, graphs or symbols, etc. For example, Data might include the names, ages, and other personal information of the individuals.

Data is important in many ways:

- The large collection of information about people's online habits has become an important source of profits.
- Governments and political parties have also gained interest in the data, and they use these sets of data for elections and policymaking.
- The data which is available online about individuals help the companies to use it and to target advertisements for us.

WHAT IS DATA LOCALIZATION?

Data Localization is the act of storing data within the territorial boundaries of the country. In other words, it means storing the data locally to prevent it from leaking personal information.

CATEGORIES OF DATA LOCALIZATION

Broad Localization-It covers the personal data from a broad perspective which means it covers all the categories of personal data and it stores a copy of the data within the country.

Specific Localization -It covers specific categories of personal data and it includes only a certain type of organization that must comply with it and the copy of the data must be stored locally.

Combined Localization-It covers the specific categories of personal data and further this type of localization does not require storing a copy of the data locally.

WHY DATA LOCALIZATION IS NECESSARY FOR INDIA?

Protection of personal data - Localization of Data is a very important aspect in the political arena since the modernization of the political world. The latest trend that is prevailing in the market is 'Data is the new oil' meaning thereby that data can prove to be the treasure of an economy. At the outset of the current data scandals, governments around the world have started to realize that the protection of data is in the hands of the country itself and now it has become an absolute requirement. It will protect the individual's data from fraud and cyber-attacks.

Law enforcement - If we store the data in our local vicinity, it can ease the access of such information by the authorities when they require it. Moreover, storing data locally is crucial for Law Enforcement. It will be beneficial for government agencies to track the data of the individuals if stored within territorial boundaries. If such information is not stored locally, then these agencies acquire data with the help of Mutual Legal Assistance Treaties (MLATs)[1], which authorize them to obtain the information access.

To prevent foreign surveillance - Storing data locally is important to prevent the data from the hands of foreign entities. If data moves outside the country, then it becomes the main concern in the aspect of leaking the personal information of individuals. For example – Big corporates like Amazon, Facebook, and Google store the data of individuals outside the country which can further cause cyber-attacks. So, to prevent the data from foreign outreach, the data is stored locally.

Growth of the local ecosystem - Storing the data locally can boost our local economy by generating employment opportunities. The major growth can be seen in the sectors such as e-commerce and financial services. For example- From data collection to data processing being done in the home country, then the manpower is required to do the work which is related to maintaining the data.

Boost India's renewable energy - Till now, the data is being stored in the data centre of foreign countries which consumed so much energy. And data centres consist of large servers and coolers that are more power-consuming. Moreover, many big business giants are purchasing wind and solar farms for storing information in the data centre which can give a thrust to India's Renewable Energy sector.

Thrust to Industrial Revolution 4.0 - Industrial revolution 4.0 means the present technological era. It also deals with the changes which are brought about by smart technologies. So, Data localization will allow companies to store data within the country which will give a boost to

[1] Mutual Legal Assistance Treaties

industrial revolution 4.0 which will result in a rapid change in technology and societal patterns due to the increasing connectivity.

POLICIES THAT IMPLY DATA LOCALIZATION

The Sri Krishna Committee Recommendations - The main recommendation regarding data localization was that personal data will need to be stored on the servers which are located within India and if some data needs to be transferred outside the country, then it is subject to proper safeguards. However, the critical data will only be processed in India. Further, the committee said if the processing of personal data is to be done for the functions of the state, then it is to be processed by the government only. The committee also recommended that the sensitive personal data of the individuals should not be processed unless consent is given by the concerned individuals. This committee recommends the amendment amend section 8(1)(j) of the RTI act[2] that pertains to the disclosure of personal information in the larger public interest.

RBI'S Directive on Data Localization - If we go back, RBI published a circular on 6th April 2018 stating that payment service providers must set up local servers. The payment service providers were opposing it because of the cost incurred. Majorly, it was being opposed by global companies. Apart from the cost, the companies like Visa and Mastercard will also be impacted by it. Moreover, RBI does not want other countries to store Indian data and it will stick to its data localization directive. RBI has imposed a hard data localization mandate on the payment system providers to store the payment system data only in India.

WHAT COULD BE THE RBI'S ACTION ON THE COMPANIES THAT FAIL TO COMPLY?

First, the companies will be submitting their audit reports and many of these companies would end up saying that we are not ready to set up the local servers. When the local servers will get set up, then the consumers using payment services won't be impacted. It further lays the groundwork for a stringent data protection bill. Draft National Digital Communications Policy 2018- First, this policy deals with the regulatory and developmental changes in ICT. This policy

[2] Right to Information Act 2005, s 8(1)(j)

has also set the goal of data localization. The main purpose of this policy is to secure the interests of citizens and safeguard the digital sovereignty of India with a focus on ensuring privacy and security. It is also dealing with its commitment towards ensuring the data protection regime. As the privacy of individuals is the main concern in today's era, so ensures safety by having a strict compliance system.

Draft Personal Data Protection Bill, 2018 - Apart from the other important aspects such as data processing and compliance, it also includes the policy related to the localizing of the data to ensure the privacy of the individuals. Further, it says that the processing of data is allowed only with the consent of the individuals. It also highlights that the individuals whose data is stored with the entities are allowed to access their data whenever they require it and can seek correction in their data. This bill allows an exemption for certain purposes like journalism, research, and legal proceedings. But these can also be questioned if they infringe on the privacy of the individuals.

The Personal Data Protection Bill, 2019 - Has recognized privacy as a fundamental right protected by the constitution. It also categorized the data into critical, general, and sensitive. It 8 states that data is to be stored within the country and if data needs to be processed outside the country, then the explicit consent of the individual is required. This bill also states that data localization in a country like India is not a welcome move because it can lead to large-scale surveillance of individuals. This bill states other alternatives to data localization like there should be better transparency standards and conditional transfer of data etc.

Data Protection Bill, 2021 - This bill has talked about data localization, and it has emphasized the issues like India's national security, privacy, and building a domestic data economy. Clause 33[3] and Clause 34[4] of the 2021 bill provide for data localization and conditional cross-border data transfers. The report which is provided in this bill has recommended the formulation of a comprehensive Data Localization policy. Further, it has recommended that some crucial steps need to be taken by the government to bring sensitive data from foreign entities to India. This

[3] Data Protection Bill 2021, cl 33
[4] Data Protection Bill 2021, cl 34

bill states that data localization is not new to India, many countries have adopted it like the USA, Russia, China, Australia, etc. This bill also states some negative aspects of data localization like it will increase the cost of the business and lowers the long-term competitiveness. Personal Data is collected from Data principles online and personal data that is collected is digitized which would govern all personal data. It will also include non-personal data.

ISSUES RELATED TO DATA LOCALIZATION

Lack of proper infrastructure - In developing countries like India, there is a lack of proper infrastructure required to collect and manage data. This may make the data prone to cyber-attacks. Localizing data can prevent foreign threats but it cannot escape the risks that are involved in the domestic storage of data. Inadequate infrastructure can lead to security issues

Huge financial stress - If we take the case of the developing countries, then the companies specifically the start-ups there will face huge financial stress since data localization requires additional investment, in the form of servers, generators, and personnel, etc.

High operational cost - If storing data is to be adopted within the country, then the government has to work on its effectiveness and its functioning which will entail a high operational cost. This will in turn put an extra financial burden on the government.

Act as a restrictive trade barrier - It states that it puts a restriction on e-commerce activities. As we know that e-commerce allows us to order anything around the world just with a click of the mouse and with an internet connection. But data localization is a main hindrance in it because it puts a restriction that affects the cross-border data flows and internet-enabled services.

Issues related to privacy - It is to be noted that data localization may not be able to eliminate cyber-attacks. Even when, Data is stored locally, it is prone to cyber-attacks leading to data breaches and loss of privacy. As cyber attackers can misuse the personal data of individuals to their advantage.

Issue related to social and economic impact - The issues which are related to social and economic impact are the most common concerns about data localization.

These concerns include:

- The cost of local employment and infrastructure investment.
- The increase in the compliance cost.
- The cost of efficiency losses such as skill dilution.

STATUS OF DATA LOCALIZATION IN OTHER COUNTRIES

European's union does not allow all the data to be localized, but it restricts flow to other countries with a strong data protection framework. So, European Union states that Data localization is unnecessary. There are many other cheaper techniques to solve the underlying problem. Further, it uses the GDPR adequacy technique which means that data can be transferred to other countries based on their adequacy status.

China - The China government makes it mandatory for all the important data to be 'Localized'. Further, it states that if any data is to be transferred outside the country, then it will undergo a strict security check. In a country like China, the data is strictly controlled by the government.

U.S.A - The U.S.A. does not have any laws relating to Data Localization for protecting user data. They don't have any localization laws at the federal level, only individual laws exist in their country such as the health insurance portability and accountability act, of 1996, etc.

Vietnam - The Vietnam government states that the data operators should retain a copy of the personal data for a specified period, and it says that the foreign companies which are engaged in Data Localization should have their branch office in Vietnam.

Indonesia - The government directive 82 of 2012 has majorly established that all the operators which are dealing with public services must set up a data centre in Indonesia itself. "Public services" here mean the services which are being offered to the public.

Russia - It has stricter laws about the cross-border flow of data and it emphasizes keeping the data within the country.

So, from the above practices which are being followed by the different countries, it can be concluded that:

There is a need for a long-term strategy and a deep analysis needs to be done for the process of Data Localization. However, many big corporates are not willing to welcome such a change in the Data Protection Framework. Further, the government should take all the necessary steps to bring such a change so that it does not cause any damage to the economy.

THE FUTURE OF DATA LOCALIZATION IN THE GLOBALIZED WORLD

If we consider the era of the globalized world, it means interconnection with different countries. So, in the globalized era, the importance of data is increasing. Governments are putting more restrictions on the flow of data across borders. The companies are forced to host the information in their home country to ensure data privacy, national security, and the protection of MSME Industries. Moreover, if the data is held within the country, then it becomes easier for the government to monitor and regulate the data. On the other hand, some business entities will miss out on great business opportunities because of the restrictions placed on the free flow of data. The future of data localization is mainly dealing with the data to be stored locally and if some global companies are transmitting the data outside the country, then it must comply with the data security requirements.

WAY FORWARD ON DATA LOCALIZATION: CONCLUDING REMARKS

The above article has made clear that data localization is a very complex and multidimensional phenomenon. Both the necessity and the issues related to data localization are very diverse and beyond the concept of data privacy. From the above, it can be concluded that there is a need for a long-term strategy for data protection and many researchers believe that data localization can be done. The government should take the necessary steps so that both the business entities and consumers are not affected much. Further, sufficient attention must be paid towards improving the infrastructure and a proper policy must be made to deal with cybercrime issues. One should conduct a full-scale assessment to understand the exact requirements of the process of localizing the data. Proper budgeting and planning must be implemented to reap the benefits of data

localization. There must be an undertaking of the actual data migration and the operations must be set up securely. As data localization requirements become more common across geographies, companies need a process to address them systematically.