IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA LOCALIZATION AND DATA PORTABILITY: ANALYSED WITH INDIAN PERSONAL DATA PROTECTION BILL, 2018 AND EUROPEAN GENERAL DATA PROTECTION REGULATION, 2018

Adv Prashant Mali, Ph.D., Founder & President - Cyber Law Consulting(Advocates & Attorneys)

Abstract

In the past five years' Indian economy had witnessed a tremendous change with the introduction of 'Digital India' and increase in the use of digital economy post demonetization. Post Aadhar and privacy judgement (K.S. Puttaswamy and Anr Versus Union of India, 2017) in India, there was a need for the regularisation and a legal framework for data protection and its related aspects. It was in this context, that Justice B.N.Srikrishna Committee was set up to look into the issue of data privacy and protection. Based on the recommendations, the Parliament came out with the draft Personal Data Protection Bill,2018 on July 27, 2018. The bill came only a few weeks after the General Data Protection Act, 2018 enacted by European Union came into force. Given the fact that the scenarios and the history behind the enactment of both laws were different, there are similarities and dissimilarities. The paper will focus specifically on the aspect of data localisation and data portability with respect to both the laws. Keeping the two in mind, it will study whether the proposed legislation in India is disguised in nature with reference to the sovereign's ultimate right over the data. It will also critically analyse GDPR's stand on data localisation and its conflict with its member countries like Germany, France and Bulgaria.

Keywords - data localisation, data portability, personal data, data protection, data transfer, privacy, privacy law, data protection law

1. Introduction

Data has become a national asset for every nation (Draft National E-commerce Policy, 2019) and personal data of citizens has become a point of concern for every government. Personal data is any data that identifies with a recognized or recognizable living person. Various snippets and pieces of data, which gathered together can lead to the identification of a specific individual, additionally comprise personal data. The term 'personal data' has been used **291** times in IN-PDPA Bill and section 3(29) of the bill defines personal data as *"any information which renders an individual identifiable."* Article 4 of (EU-GDPR, 2018) also defines 'personal data' as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location*

data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

1.1 Data Localisation: Data Localisation is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated. The term "Data Localisation" has neither been used nor defined under IN-PDPB as well as EU-GDPR. But the related provisions have been mentioned in IN-PDPB discussed in detail later.

1.2 Data Portability: Data portability refers to the ability to move, copy or transfer data easily from one database, storage or IT environment to another. Portability describes the extent to which the data can easily be ported between different computers and operational environments. "Right to Data Portability" has been defined in both IN-PDPA as well as EU-GDPR. One of the aims of data portability is to allow more competition into the market.

1.3 The Personal Data Protection Bill, 2018 and its features-

India has the second largest number of internet users but still did not have the data protection framework until recently. The Supreme Court's judgement on "Right to Privacy" emphasised on the needs of the data protection and hence the Bill came based on the recommendations of the Justice B.N. Srikrishna Committee.

- The Personal Data Protection Bill ensures protection and regulation of personal data of individual known as data principal by the government and private entities known as data fiduciaries.
- An individual's personal data which can be used to identify him/her should only be processed with his/her consent under certain conditions and safeguards.
- The fiduciaries have certain obligations towards the data principal while processing their data, such as notifying them of the nature and purposes of data processing.
- Certain kind of exemptions are also allowed by the IN-PDPB bill for data processing, such as processing for legal proceedings, journalistic purposes and in the interest of national security.
- The bill ensures that at least one copy of the personal data should be stored within the territory of India and certain sensitive and critical personal data should be stored only in India.
- Certain rights are given to the data principals u/s 24,25,26 and 27 namely Right to confirmation and access, Right to correction, Right to Data Portability and Right to Be Forgotten.
- A national-level Data Protection Authority (DPA) is set up under the Bill to manage, supervise, regulate and control data fiduciaries.

1.5 The Reserve Bank of India Guidelines on Data Localisation-

When the draft IN-PDPB bill was in process by B.N. Srikrishna Committee, the Reserve Bank of India issued some guidelines for data storage and data localisation on April 6, 2018 via its notification RBI/2017-18/153 addressing all banks, authorised payments systems and all financial institutes to store all payments related data only on Indian servers and data centres which are located in Indian Territory only. These directives were applicable not only to payment entities but also to all banks operating in India (Reserve Bank of India, 2018).

- The reason given by RBI for this data localisation was for "better monitoring" and for its unfettered supervisory access to data stored with these system providers.
- All the system providers were given deadline till October 15, 2018 for implementing these data storage and data localisation guidelines. Some of the big giants in payment system providers like "VISA" haven't fulfilled and implemented these guidelines till 2019 and asking for extensions.
- System Audit Report(SAR) done by professionals empanelled with CERT-IN was also to be submitted to RBI by December 31, 2018 which most of the system providers failed to do so.
- On April 26, 2019 the Reserve Bank of India issued clarifications on their earlier notification of 'Storage of Payment System Data' advising all system providers to ensure that, within a period of six months, the entire data relating to payment systems operated by them is stored in a system only in India.
- Through this clarification, RBI made this clear that there is no bar or restriction on processing of payments transactions outside India if so desired by the payment system operators (PSOs) however that data shall be stored only in India after the processing. PSOs can take one business day (i.e.) 24 hours time frame to bring back payment data processed outside India.

- The payment data sent abroad for processing should be deleted abroad within the prescribed time line and stored only in India. The data stored in India can be accessed / fetched for handling customer disputes whenever required.
- In the case of banks, especially foreign banks, earlier specifically permitted to store the banking data abroad, they may continue to do so; however, in respect of domestic payment transactions, the data shall be stored only in India, whereas for cross border payment transactions, the data may also be stored abroad as indicated earlier.

1.6 The EU-GDPR and its features-

The General Data Protection Regulation is a law adopted by the European Union and the European Economic Area on data protection and privacy for its citizens. It also addresses the export of personal data outside the EU and EEA areas.

- The EU applies its jurisdiction to any personal data processing, in the EU or abroad, that originates in the EU. The EU-GDPR shall apply to all data controllers and processors established in the European Union (EU) and organizations that target the EU citizens outside of the EU.
- The GDPR also establishes penalty rates for noncompliance, rules on user consent, data erasure, breach notification, right to access, and data portability. But importantly, the GDPR allows for the flow of data to third-party countries if the receiving country's laws are in compliance with the GDPR's rules.

- Certain rights are given to the Data Subjects under Article 15,16,17,18,20 and 21 including Right to restriction of processing, Right to be forgotten and Right to Data Portability.
- The General Data Protection Regulation (GDPR) has taken a hybrid approach towards data localization. The most essential feature of GDPR is that it does not restrict the flow of data to third countries but merely imposes conditions and extends its jurisdiction to any personal data processing, in the EU or abroad, that originates in the EU.

2. Data Localisation in Context Of PDPB :

Personal data of every individual has become the latest buzzword. The Reserve Bank of India's Data Localisation guidelines dated April 6, 2018 were made to ensure the implementation of Data Localisation by companies like Visa, MasterCard, Facebook, Whats App, Amazon, Alibaba and many more. The data of transactions done in India should remain in India and not be backed up some other data centres outside India. The fact is true that India neither defined the term 'data localisation' nor this term has been used anywhere in the draft Bill. But laws and certain restrictions on data localisation, data storage and cross-border transfer and overseas storage of data have been provided in the draft. Restrictions and Conditions for cross-border transfer of personal data has been defined U/S 40 and 41 of Personal Data Protection Bill (Deloitte, 2018).

- As per S.40(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, or at least one serving copy of personal data to which this Act applies.
- Under S.41 of IN-PDPB, it has been stated that 'Personal data other than those categories of sensitive personal data notified under subsection (2) of section 40 may be transferred outside the territory of India where the approval is mandatory by the Authority.'

2.1 Data has been categorized in 3 different types :

- Personal Data : Data about a natural person in relation to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features with any other information.
- Senstive Personal Data : Sensitive personal data includes passwords, financial health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation.
- Critical Personal Data : Under Section 40(2), it has been provided that categories of personal data as critical personal data shall be notified by the Central Government which shall only be processed in a server or data centre located in India.

2.2 The Push for Data Localisation :

The most basic ground on which the Indian Government is pushing Data Localisation is for Securing Citizen Data.The government argues that storing and processing data locally will secure Indian users' data and make service provider that stores such data more accountable. Data Localisation will also provie more privacy leading to Data Privacy and Data Sovereignty. National Security is a big concern for every step a nation takes for its development, rise and upliftment. As India moves towards becoming a global hub for the digital technology. This move would give a push to the Indian businesses.

2.3 Arguments against Data Localisation :

1.) Security Concern : With all the data stored locally it creates a possibility of data breach by various stakeholders concerned both inside and outside the country. If lost, it will be a direct threat to the country's financial and physical security.
2.) Structural Issues-
a) Implementing the required infrastructure will come at a very high cost and will also require a full upgrade of existing facilities and hardwares.
b) Need of 24x7 electricity, high human resource for the maintenance.
c) Feasible geographical conditions offered by a small portion of the country.
3.) Data Localisation in someway or the other will not be a shield to the personal data but a weapon for the Law Enforcement and Investigating Agencies. The same has been elaborated later.

2.4 Data Localization as a weapon for Law Enforcement Agencies:

Data Localization in India will not act as a shield to a data subject's personal data but it will be a weapon for the Law Enforcement Agencies and Investigating agencies. Right now, it is very difficult for such agencies of India to take or ask for data from foreign countries for the purpose of investigations and digital evidence collection (Bailey, Bhandari, Parsheera & Rahman, 2018). Big Giants like Facebook, Google, WhatsApp, Instagram, Microsoft etc. take about 10-15 days for just providing the IP address of the user and in the cases where IP is masked by the user or some foreign proxy is used by user, companies even deny to provide the data and ask Law Enforcement Agencies to come through the channel of MLAT (Mutual Legal Assistance Treaty). Making investigation through MLAT is a cumbersome take and take years leaving the investigation agencies helpless in the cases of heinous crimes like Murder, Rape, Kidnapping etc.
WhatsApp calling has become the most common modus-operandi for asking ransom in the cases of kidnapping and abduction. In these types of cases, action should be taken by the Law Enforcement Agencies in very less time which requires quick response from WhatsApp but the company takes minimum 8-12 working hours to respond to emergency requests and sometimes deny to provide user's data (IP Addresses, Device Details, Mac Address, IMEI number etc.) to the Law Enforcement Agencies (Bailey, Parsheera, 2018).
To deal with these situations and to overcome these problems, the draft PDPA Bill S.40(1) ensures that:
S.40(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

The Bill's mandate on data localization is one of the most-watched provisions by foreign technology companies. The panel on data protection, which took almost a year to prepare its report and the draft bill, had recommended that a copy of all personal data should be stored in India, while all information of a critical nature could only be kept locally.

2.5 Feasibility of Data Localization in India :

1. India is located at the center of trans Indian ocean routes which connect the European countries making it easier for India to be connected to other countries which would be beneficial for transferring of huge devices and for installation of undersea cables.
2. Since India is covered by oceans on three sides, electricity generation from tides is one of the boons. In the recent budget of Gujarat (2019), Gujarat is targeting 30GW renewable capacity by 2022 which will be a huge source of electricity for data centers. Gujarat can become a hub for Data Centers and Cloud Services (Verma, 2019).
3. Due to large coastline of India transportation, communication and trade becomes very easy.
4. India is divided by the Tropic of Cancer in two parts making upper half cooler and lower half tropical climate. Both the halfs can be used in its own way. The sub-tropical upper half can be used to establish data centers as it is cooler and less humid. The fats blowing winds in the region can be a good source of wind energy which can be used to produce electricity. For the tropical lower half region which covers the South India, tidal energy can be a viable option.
5. India is said to be 7thlargest country in terms of landmass and accounts for 2.4 % area on the globe which is huge. Data centers require huge amount of space or area to be established and can be provided by the country easily.
6. Huge Cloud Server giants Amazon Web Services(AWS), Microsoft Azure Cloud Computing Services and Google Cloud Services has established their data centers and cloud servers at Mumbai, Pune, Chennai and Hyderabad already for "Infrastructure-as-a-service","Business-process-as-a-service"and"Software-as-a-service".
7. India already has few indigenous data centers existing like CrtlS, Reliance, TATA, Net4 and so on.

2.6 Criticism of data localization w.r.t. PDPB by EU and U.S. :

The European Union says that 'These data localization requirements under IN-PDPA bill appear both unnecessary and potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments'(Gencarelli, 2018).

India is planning to grow its economy to 1 trillion US Dollars in the next 4 to 5 years. U.S. Tech Giants are opposed to localization of data in India because it will cost them a lot. The U.S. has termed India's move to restrict cross-border data flow and strict e-commerce rules as *"discriminatory and trade-distortive"*.

The US Trade Representative says that "India has recently promulgated a number of data localization requirements that would serve as significant barriers to digital trade between the US and India"(Lighthizer, 2019)

The main reason behind this criticism is that the U.S government doesn't want its big giants including VISA, Facebook, WhatsApp, Instagram, YouTube, Google to store their data on data centers in the Indian territory. The issue of infrastructure, cost and maintenance is not so big for these giants as it has been portrayed to be. Fiduciary bodies can manage storing data in India through infrastructure by leasing "wholesale" data center space to third-party landlords. Wholesale providers build the data center, including the raised-floor technical space and the power and cooling infrastructure, and then lease the completed facility (CBRE, 2016).

3. Data Localization in Context of EU-GDPR :

The old joke goes that "cloud is just someone else's computer" but what if you don't even know where that computer is located. Data Localization concerns about the location of that computer. Data is the 21st century's oil, says Siemens CEO Joe Kaeser. This means that the world's most valuable resource is no longer oil, but data and every country would like its most valuable resource to be presented in its own territory. GDPR doesn't limit the flow of data to third countries however only forces conditions and stretches out its jurisdiction to any personal data processing, in the EU or abroad, that originates in the EU (Reinsch, 2018).

The General Data Protection Regulation(GDPR) has taken an implicit approach towards data localization. The shape of export restrictions on data are designed in such a manner that personal data cannot be exported outside of the European Economic Area (EEA) unless the recipient non-EEA country has either been deemed by the European Commission to offer adequate data protection safeguards or a valid export mechanism has been put in place (e.g. Commission approved model clauses or Binding Corporate Rules). Failure to comply with the export rules can attract Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements as fine (Osterman, 2017).

Under Article 44 and 45 of the Act, law for "Transfers of personal data to third countries or international organizations" is explained. The law and the rules framed under EU-GDPR are so harsh and strict against data infringement that a data fiduciary or a foreign country will think twice before establishing a data center which stores European citizens' data in its territory. Nonetheless, most cross-border transfers of personal data will be done under standard legally binding contractual clauses as there are just a couple of nations with a vigorous data protection and assurance regime. Indeed, even the EU has recognized just 12 nations to have ampleness status under the GDPR (Khaitan & Co., 2018).

In particular, the GDPR states that personal data must be moved to nations outside the EU when a satisfactory degree of security is ensured. In the event that an organization has even the scarcest uncertainty about a specific goal, the data can't travel there. With the cost of non-compliance so high, many enterprises will select to avoid any risk, by guaranteeing their client data remains inside the EU, or even within the country of origin. Germany, for example, denies sharing data over the national outskirts (even inside the EU) without ensured insurance levels (Synytsky, 2017).

3.1 Article 27 of EU-GDPR :

Article 27 of EU-GDPR talks about "Representatives of controllers or processors not established in the Union". Data fiduciaries who are storing personal data of EU data subjects in data centers/servers/cloud which are outside Europe have to assign a representative. As per Article 27(1), the controller or the processor shall designate in writing a representative in the Union. Article 27(2) says that the representative shall be established in one of the Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored (EU Regulations, 2016) . GDPR requires data fiduciaries to have a local representative. The purpose being, in case any foreign data controller or processor deny to give data to the state, in that case the state can arrest the local representative which can be regarded as a better approach for the government to force corporations to submit data. In some way, this approach is better than bringing up the whole data localization concept. However, there are some member countries of EU which implements data localization explicitly as per their regional laws.

Following table shows restrictions to cross border data flows and countries with sector-wise data localization (Digital Trade Estimates, 2019):

Country	**Act, Code, Practice**	**Description Measure**
Bulgaria	Gambling Act	In Bulgaria, a candidate for a gaming permit must guarantee that all data related to operations in Bulgaria is stored on a server situated in the geographical location of Bulgaria. In addition, the candidate needs to guarantee that the correspondence hardware and the central computer system of the coordinator are situated inside the EEA or in Switzerland.
France	Ministerial Circular 5 April 2016 - Note d'information du 5 avril 2016 relative à l'informatique en nuage (cloud computing)	A ministerial circular dated 5 April 2016 on public procurement states that it is illegal to use a "non-sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France.
Germany	German Telecommunications Act, as amended in December 2015	In October 2015, a new data retention law was passed, which entered into force in 2017. The law provides that telecommunication providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany only (§113b).
Greece	National Law 3917/2011	In Greece, the National Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later repealed by the European Court of Justice) by requiring that retained data on 'traffic and localisation' stay 'inside the premises of the Hellenic region'. The law is still in force.
Luxembourg	CIRCULAR CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597	According to the Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.
Netherlands	Public Records Act	Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies to both paper and electronic records. Electronic records can't be stored on any server located outside the Netherlands.

Poland	Polish Gambling Act	As indicated by the Polish Gambling Act, any element sorting out gambling exercises is obliged to file all data traded between such entity and the clients in an archive gadget located in Poland progressively. Another limitation is the necessity that the hardware (servers) for preparing and putting away data and information with respect to the bets and their participants must be installed and kept in the geographical territory of the EU or EFTA.
Portugal	Data Protection Law	On 10 November 2015, the Portuguese Data Protection Authority (DPA) also issued specific guidelines on Intra-Group Agreements ("IGA") involving transfers of personal data to non-EEA countries. The DPA considers that such transfers depend on prior authorization for the purposes of assessing if IGAs contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EEA countries.
Romania	Law no. 124, May 2015, regarding the approval of the Government Emergency Ordinance no. 92/2014 regulating fiscal measures and modification of laws	In Romania, the game server must store all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out. Information must be stored using data storage equipment (mirror server) situated on Romanian territory.

4. Data Portability in context of IN-PDPB:

- Under section 26, the data principal has "Right to Data Portability" through which a data principal can ask for his data which he has provided to the data fiduciary, data generated in the course of provision of services or the data which forms part of any profile on the data principal in a structured, commonly used and machine-readable format.
- Under section 26(1)(b) of the PDPB bill, the data principal has been provided with a right to transfer its personal data from one data fiduciary to another data fiduciary in the format referred to in section 26(1)(a).
- The right to portability is a key step towards empowering consumers to unreservedly choose and migrate their data across service providers. While we recognize that data fiduciaries/entities would face technical challenges in facilitating such requests, the bill allows fiduciaries to charge a reasonable fee and restricts the scope of such requests to personal data obtained consensually and processed using automated means (Vishwanath, 2018).
- Under section 26(2), it has been stated that processing of data shall only be applicable where the processing has been done through automated means and shall not apply in three conditions. The third condition says that data processing shall not be applicable where "*compliance with the*

request that would reveal a trade secret of any data fiduciary or would not be technically feasible."

- The grounds of technical feasibility have not been justified in the bill. Eg. If a user wants to transfer the location history from an application that only runs on ios platform to an application that only runs on android platform, it can be technically feasible to make the processing and the transfer. In second case, if a user wants to transfer his messages from one application that runs on ios platform to another application that also runs on ios platform, the transfer and the processing cannot be technically feasible.

4.1 Interoperability:

One important concept alongside data portability is "Interoperability". Interoperability refers to the compatibility with sharing. It also refers to the extent to which one service provider's infrastructure can function with other service provider's infrastructure. In software terms, interoperability is usually implemented through Application Programming Interfaces (APIs)—interfaces that allow other developers to interact with an existing software services. For example, Cab booking service providers like Ola, Uber etc. works on interoperability with Google Maps. Prior to the Aadhar and privacy judgement (*K.S. Puttaswamy and Anr Versus Union of India,2017)* telecom companies and ISPs used to call UIDAI Application Programming Interfaces (APIs) for porting and fetching user data from Aadhar Card database. The Aadhar authentication API used to return all the data including name, age, address, photograph and biometric data as a part of response to the service provider. But post judgement, Data Portability and Interoperability got suspended and UIDAI revised their norms of Aadhar Authentication API calling and now Aadhaar authentication service only responds with a "yes/no" and no personal identity information is returned as part of the response (UIDAI, 2017).

5. Data Portability in Context Of EU-GDPR :

Data portability is a right which allows you to ask your online service provider to either have you download all your data or ask them to transfer your data to another online service provider you want to use.

Users in Europe can simply visit online service provider's website and click on the "DOWNLOAD" button to download their data. The data sent to the user is in commonly used machine readable structured format which means that when the user move the data, the structure around the data should remain same but both of the service providers should have similar kind of layout in order for the pictures, posts, emails etc. to be displayed in the same way. For instance, if any user moves a post from Facebook to Twitter, because of the character limit, the post might appear completely different. With "Right to Data Portability", The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Scope of this new right :

- Processing must be based on consent or on a contract and carried out by automatic means.
- Right to receive the personal data concerning him or her in a structured and commonly used format and have the right to transmit those data to another controller without hindrance.
- Data subjects have the right to have the data transmitted from one controller to another controller where technically feasible.
- The GDPR encourages online service providers to get together and agree on some kind of intra-operational database format.

6. Feasibility and Critical Analysis of Data Portability :

Both the EU and the Government of India have given the "Right of Portability" in GDPR and PDPA to the data principal and data subjects but the question arises "Is the Data Portability as easy and feasible as it appears to be?" The answer is no. Both the legislatures had said that "Users can transmit their personal data from one data controller or from one fiduciary body to the other wherever technically feasible". Data Portability always bring competition in the market and the society. Now, if a data subject uses Facebook in 2019 and a rival company came into the market let say "Wholebook" in 2020 and starts offering more features and services to its users. Then, all the users of Facebook would like to shift to Wholebook and at that time, 'Will Facebook port all the data of its users to Wholebook?' No, the company will be having a strong defence of 'technical feasibility' as no data fiduciary would like its users to get transferred to any other service provider.

7. Conclusion:

While analyzing Data Localisation and Data Portability with EU-GDPR and IN-PDPB bill, it has been clear that "Data is a national asset" and every country wants its national assets to be protected. EU has made regulations and laws so harsh that any foreign country will think twice before storing data of European data principals in its territory whereas India has shown an explicit approach towards the Data Localisation. EU-GDPR has set an example for the other data controllers after imposing a record breaking fine of 183 million pounds on British Airways for data breach on July 8, 2019. In the current scenario, the EU approach against data breach and sector-wise localisation by member countries of the EU seem to be a better approach than India's direct approach towards the data localisation but the Government of India might have understood the future need of data localisation. In so many articles and newspapers, experts have said that 'Next World War will be a Cyber War' instances of which can be clearly seen from the recent Iran vs. U.S. battle and 'Data' will play the most important role in the Cyber War and implementing 'Data Localisation' is a big concern for National Security which should be implemented immediately. Keeping this in mind, India's direct approach is commendable. 'Technical feasibility' is still a big point of concern for both GDPR and IN-PDPA bill. To make data portability applicable fairly and to make the citizens enjoy the 'Right to Portability', the government should make certain guidelines for the development platform of an application. The format in which data fiduciaries stores data of data subjects should become centralized for making 'Right to Portability' as a fair and equal right for all data subjects.

References

Justice K Puttaswamy (Retd.) and Anr. v Union of India and Ors 2017 Indlaw SC 641 retrieved from https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Draft National E-Commerce Policy, 2019 retrieved from https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

Indian Personal Data Protection Bill, 2018 retrieved from https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

European General Data Protection Regulation, 2018 retrieved from https://gdpr-info.eu/art-4-gdpr/

Report of B.N Srikrishna Committee, 2018 retrieved from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Sindhu Balaji, 2018, *India Finally has a Data Privacy Framework – What does it mean for its Million Dollar tech Industry* retrieved from https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#662eac0a70fe

Reserve Bank of India Notification DPSS.CO.OD No.2785/06.08.005/2017-2018 retrieved from https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.pdf

Reserve Bank of India, FAQ on *Storage of Payment System Data* retrieved from https://rbi.org.in/Scripts/FAQView.aspx?Id=130

Deloitte,2018, *India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation* retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf

Bailey, R., Bhandari, V., Parsheera, S. & Rahman, 2018. *Use of personal data by intelligence and law enforcement agencies'*. National Institute of Public Finance and Policy. retrieved from http://macrofinance.nipfp.org.in/PDF/ BBPR2018-Use-of-personal-data.pdf

Aditya Kalra, 2018, US senators urge India to soften Data Localisation stance. Reuters retrieved from https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN

Rishab Bailey and Smriti Parsheera, 2018, *Data Localisation in India: Questioning the Means and Ends* retrieved from https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf

Ayush Verma, 2019, *Gujarat Targeting 30 GW Renewable Capacity by 2022* retrieved from https://www.saurenergy.com/solar-energy-news/gujarat-targeting-30-gw-renewable-capacity-2022

Bruno Gencarelli, 2018 *Submission on draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY)* retrieved from https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en

Robert E. Lighthizer, 2019, *National Trade Estimate Report on Foreign Trade Barrier*s retrieved from https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf

CBRE, 2016, Writing The Next Chapter in The Asia Pacific Data Centre Evolution retrieved from https://www.missioncriticalmagazine.com/ext/resources/MC/2018/Jan-Feb/APAC_Major-Report---Writing-the-Next-Chapter-in-the-Asia-Pacific-Data-Centre-Evolution_September_2017.pdf

William Alan Renisch, 2019, *A Data Localization Free-for-All?* retrieved from https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all

Osterman, 2017, *GDPR Compliance and Its Impact on Security and Data Protection Programs* retrieved from https://4b0e0ccff07a2960f53e-707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/wp-

content/uploads/2017/02/GDPR-Compliance-and-Its-Impact-on-Security-and-Data-Protection-Programs-HPE.pdf?v=20

Francesca, 2018, *Digital Trade Restrictiveness Index* retrieved from http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf

Khaitan & Co., 2018, *India: Decoding The Personal Data Protection Bill, 2018*, retrieved from http://www.mondaq.com/india/x/727776/data+protection/Decoding+The+Personal+Data+Protection+Bill+2018

Ruslan Synytsky, 2017, *GDPR and Data Localization: The Significant (and Often Unforeseen) Impact on the Cloud* retrieved from https://www.scmagazine.com/home/opinion/executive-insight/gdpr-and-data-localization-the-significant-and-often-unforeseen-impact-on-the-cloud/

Regulation (EU) 2016/679 of the European Parliament retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Digital Trade Estimates (DTE) Database retrieved from www.ecipe.org/dte/database

Siddhart Vishwanath, 2018, *Decoding the Personal Data Protection Bill, 2018 for individuals and businesses* retrieved from https://www.pwc.in/consulting/cyber-security/blogs/decoding-the-personal-data-protection-bill-2018-for-individuals-and-businesses.html

Unique Identification Authority of India, 2017, *Aadhar Authentication API Specification – Version 2.0* retrieved from https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf