Section: Research Paper
ISSN 2063-5346

Significance of Data Localisation in Data Protection-An Analysis

Vidhya Praveen Shetty
Research Scholar
AKK New Law Academy, Savitribai Phule Pune University, Pune and
Assistant Professor, Department of Law, Tilak Maharashtra Vidyapeeth, Pune.

Dr Harunrashid A Kadri
Professor of Law &; Principal I/c
G. E. Society's N. B. Thakur Law College, Nashik,
affiliated to the Savitribai Phule Pune University, Pune.

Abstract

In this era of modernization and technological developments, the Internet has become indispensable. The internet creates and stores a huge amount of data that may be purchased and sold within and outside the geographical boundary. However, due to its flow and storage beyond the boundaries, it becomes difficult for the state machinery to regulate and monitor its use by the enterprises engaged in its collection and analysis. This makes the data prone to commercial exploitation for economic gains even without the consent of the individuals to whom it belongs, affecting their privacy, life and personal liberty. Due to the increasing exponential industrial value of data, government bodies attempt to protect their citizens data rights. The data protection regulations ensure the security of individual's personal data and regulate the collection, storage, usage, transfer, dissemination and disclosure of the data. However, cross-border data storage prevents domestic law enforcement agencies from accessing such data and surveillance of data becomes difficult. Ultimately, the state authorities fail to prevent foreign companies from unauthorised economic gains through the exploitation of such personal data, unauthorised use of personal information and privacy invasion. Therefore, to tackle the challenges raised by the cross- border transfer of data, many countries have attempted to control and protect data transfers through various modes. Data localisation is one such option whereby data protection is sought by the countries. Data localisation refers to the legal requirements for the storage of data, copying of data within the territorial boundaries of a country or/and any restrictive measures on data transfer beyond the national borders. The present paper is aimed at analysing how data localization plays a significant role in Data Protection. The researchers have examined the right-based approach to data localization in the European Union and the choice-based approach to data localization in the United States while discussing the measures to be adopted by India for better data protection in this digital world.

Keywords: Data Regulation, Data Protection, Data Localisation, Data security, Cross border data transfers.

Introduction

Exponential technological development have led the computers to handle enormous amounts of information which allows them to find connections and patterns in many spheres of human activity. Businesses all around the world have realised the potential of these databases involved in day to day activities of humans, new technology is developed to properly mine and exploit this data. Many businesses create different proprietary systems to examine this data for trends, patterns, and unnoticed nuance.Such activities sometimes do benefit the individuals in their daily lives. This is what can be termed as "Digital Revolution".This Digital Revolution has not spared India too. The Government of India has envisioned and implemented the "Digital India" plan in recognition of its relevance and the potential for significant disruptions it holds in practically all spheres of society.

As a result of Digital India project and the rise in internet usage over the past few years, there are around 692 million active users online in India as of February 2023. At this time, mobile internet users accounted for the majority of traffic in the second-largest internet market in the world.[1]India is moving quickly towards becoming a digital economy with a sizable market for international firms.In the next 40 to 50 years, it is anticipated that the digital economy would create new job prospects and market growth opportunities.

Data and its Types: A "representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means" is what the new Bill refers to as "data."[2] Data can be personal data, critical data, sensitive personal data and critical sensitive data.

Threat to Unprotected Data: Data which remains unprotected can be subjected to the following threats,

- **Continuous Online Monitoring**: Online user behaviour is frequently monitored. Although most nations require websites to inform users of cookie usage, consumers may not be aware of the extent to which cookies are monitoring their activity. Cookies frequently record a user's activities.
- **Loss of data control:** Due to the widespread usage of so many online services, people might not be aware of how their data is shared with third parties in addition to the websites they deal with on a daily basis, and they might not have any control over what happens to it.
- **Lack of transparency:** When using web applications, users frequently have to enter personal information such as their name, email address, phone number, or location. However, the privacy policies for those programmes may be complex and challenging to comprehend.
- **Social Networking:** Social media platforms make it simpler than ever to find people online, and posts on these platforms sometimes reveal more personal information than

[1]Digital population across India as of February 2023, available at https://www.statista.com/statistics/309866/india-digital-population-by-type/ (Last Modified: April 08,2023.)
[2] As per the Draft of Digital Personal Data Protection Bill,2022

users are aware of. Furthermore, social networking sites frequently gather more data than their users are aware of.

- **Cybercrime:** Numerous attackers attempt to steal user data in order to perpetrate fraud, compromise security systems, or sell the data on black markets to individuals or organisations who will use it for nefarious ends. Others seek to infiltrate internal systems of businesses that house personal data. Some attackers try to fool consumers into disclosing personal information using phishing attacks.

Need for Data Protection/Security and "Right to Privacy" in India:A rise in regulations intended to improve people's rights in the handling of their personal data has coincided with changes in the nature of global data flows. This is known as data protection, and it may be thought of as a collection of guidelines created to give people rights when it comes to the processing of information that could be used to identify them as well as to establish so that they provide potency for data processing.**Data Security** is the process of safeguarding data throughout its lifecycle from loss, theft, or unauthorised access.

To safeguard citizens' rights and foster trust in internet services, data protection law is thus very crucial. Additionally, it makes it easier to carry out important projects for benefit of the public in general because many people might be reluctant to take part in the extensive data collection that such initiatives entail in the absence of a legal framework that safeguards their privacy. In particular for a nation like India with a robust digital services sector that depends on being able to freely access data from other countries, data protection has a significant economic impact.

The Supreme Court of India acknowledged a constitutional "Right to privacy" against the State in its Puttaswamy[3]judgementof 2017. Recognizing the "Right to privacy" does not equate to having a legal framework for Data protection because data protection is a subset of the "Right to privacy" but distinct from it. Data protection law is frequently broader than privacy since it includes a larger range of data processing, even when it may not entail an individual's right to privacy.The goal of assisting in the development of a better Internet is centred on data privacy. In the information era, there are risks to privacy that can come from both state and non-state actors.

The Supreme Court of India has acknowledged the importance of the nation's international legal obligations and has advices that India should look beyond the EU and also align its data protection legislation with international standards, as well as increase its participation in international organisations like the Council of Europe and the OECD that support their development, in light of the growing recognition of data protection throughout the world.

Determining and Defining Sovereign Data Control: It would be helpful to define a number of terminologies that have been used by various parties in India and overseas in the context of sovereign control of data before we get started.Terms like "**Data Localization," "Data Residency," "Data Nationalism," and "Data Sovereignty"** have been widely used to define the conditions necessary to guarantee a country's control over the data generated

[3] KS Puttaswamy v Union of India (2017) 10 SCC 1 [157]

within its borders.There are also other terms like **"Data Protectionism" and "Data Colonialism"** which are frequently used in India and other countries to support Data Localisation.

"Data Localization," "Data residency": Both these terms are usually used interchangeably.'**Data localization' or 'data residency**' requirements are terms used to describe specifications for the local processing and storage of data. In general, the term "data localization" refers to "any legal restriction on data moving globally and compelling it to remain locally." These regulations may take many different forms. This might entail setting precise guidelines for storing copies of data locally, requiring the creation of local content, or putting restrictions on cross-border data transfers that effectively serve as a localization mandate.[4]

'**Data nationalism**' is the term for policies that aim to secure domestic sovereignty over data.[5]

"Data sovereignty" A related term is "data sovereignty," which is essentially a guarantee that national law will apply to data even if it is stored outside its borders. Some scholars have different theories of data sovereignty, which necessitate preserving data on national soil.[6]

"Data Protectionism": It may refer to the imposition of limitations on cross-border data transfers as a matter of economic policy. One component of such an agenda could be the requirement for local data storage.[7]

One of the important Technology that Protect Data is **Access Control systems** where only individuals who are authorised can access systems and data. To prevent sensitive data from leaving the network, access control and data loss prevention (DLP) can be used together. Thus these technologies thereby suggest the Significance of Data Localisation in Data Protection.[8]

"Data Colonialism": It refers to the exploitative practises of contemporary western digital firms that are comparable to the predatory colonial practises of the past and use data-driven income generation.[9]

Objectives of Data Localisation: Data localization stands crucial to many governments, companies, and individuals for a number of reasons. The primary objectives of Data Localisation are:

---

[4] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' [2013] Issues in Technology Innovation, 16.
[5] Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015), Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 (Last Modified April 06,2023)
[6] Ibid
[7] C. Kuner, Data Nationalism And Its Discontents, Emory Law Journal, 2015, Available at https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1024&context=elj-online (Last Modified April 06,2023)
[8]Available at https://www.cloudflare.com/learning/privacy/what-is-data-privacy/#:~:text=Data%20privacy%20generally%20means%20the,online%20or%20real%2Dworld%20behavior. (Last Modified April 06, 2023.)
[9] Ibid

- **Data Protection and Data security:** The desire to keep sensitive data within the boundaries of a given country in order to increase its security is one of the primary objective for data localisation. Governments and companies handling sensitive information, such as personal information, financial information, and intellectual property, may find this to be of special importance.
- **Data Privacy:**Data localisation can also be utilised to guarantee that data is governed by particular privacy laws and rules. For instance, the General Data Protection Regulation (GDPR) of the European Union mandates that personal information of EU individuals be stored and processed in a manner that assures adequate protection of their privacy.
- **Economic Development:**By requiring businesses to store and process data within their borders, several nations view data localization as a method to strengthen their own economies. This could boost economic development and generate jobs locally.
- **National Sovereignty**: Data localisation may be viewed by certain governments as a means of establishing their national sovereignty and dominance over the data of their constituents. They might believe that data kept outside their country is not subject to its rules and regulations since it is not under their control.
- **Better Performance**: Certain services, online programmes and websites, can operate better when data is kept close to consumers. In order to get faster access and lower latency, data must travel a shorter distance.

Methods of Data localisation: Data localization entails processing and storing data in a particular area. Depending on the kind and amount of data involved as well as the particular specifications of the rules and regulations that apply, there are many methods that can be used to accomplish this. Data localization methods that are often used include:

- **In-House Storage:** Keeping data on actual servers or other storage devices inside the boundaries of a country is one approach to store it locally. This may entail constructing or leasing a data centre domestically or utilising local company-owned and -operated servers and storage equipment.
- **Cloud Storage:**Another choice is to keep data in a cloud environment that is contained within a specific nation. This may entail utilising a cloud service provider with local data centres or establishing a private cloud run by a local business or organisation.
- **Data Transfer:** In some circumstances, it may be necessary to transfer data from one place to another in order to meet the demands of data localization. This may entail transferring data between various storage or processing environments or moving data between data centres.
- **Data Processing:** Processing data in a certain area of the world is another aspect of data localisation. This can entail using domestically run cloud-based processing services or local servers, storage, and other infrastructure to process data.[10]

[10] Available at https://www.imperva.com/learn/data-security/data-localization/ (Last modified April 09, 2023)

Approaches to Data Localisation: Anirudh Burman and Upasana Sharma in their working paper on How Would DataLocalization Benefit India? (April, 2021)[11] have discussed various approaches in whichData Localisation takes place

- **Strict Localisation:** This refers to enforcing legal requirements for data processing and storage within the nation, which may include complete prohibition on cross-border data transfers. Although no nation has implemented total prohibition, there are several examples of Strict Localisation. China has enforced stringent data localisation laws for sensitive data acquired by operators of essential infrastructure, including personal information. The Chinese government has strict (semi-complete) localisation standards for the financial and healthcare industries. A comprehensive and stringent localisation requirement in Vietnam's cybersecurity law mandates local data storage for all domestic and international telecommunications providers as well as for providers of internet over-the-top services. [12]
- **Partial Localisation:** Partial localisation refers to the imposition of legal requirements to store data locally; nevertheless, it does not forbid the transfer or storage of copies of the data overseas, although specific compliance requirements may be imposed for cross-border data transmission and storage. For instance, even though personal data can be moved internationally, the Russian Federation and Kazakhstan mandate that businesses keep a duplicate of the data locally. [13]
- **Conditional Transfer (Hard, Medium, Soft) Localisation:** A conditional transfer requirement denotes that data can only be moved internationally if certain requirements are met. Conditional transfers may fall under the categories of hard, medium, or soft transfers, depending on how these compliance requirements are constructed. Strict transfer permissions, rigid regulatory audits, binding company regulations, etc. are examples of hard compliance procedures. The EU GDPR is the most glaring example. Medium to soft conditions refer to simpler compliance requirements, as in the case of Mexico, where the data protection law only requires user consent and the execution of necessary contracts between data processors and the foreign parties handling the personal data when transferring personal data abroad. No other requirements for prior regulatory approval are present.[14]
- **Choice-based approach:** Choice-based approach suggest that all data, including personal data, can typically travel across borders freely with little to no legal limitations. The main proponent of this strategy is the USA. [15]

[11]Avaialble at https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291(Last modified April 09, 2023)
[12]Avaialble at https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291(Last modified April 09, 2023)
[13]Avaialble at https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291(Last modified April 09, 2023)

[14]Avaialble at https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291(Last modified April 09, 2023)
[15]Avaialble at https://globaljournals.org/GJHSS_Volume21/2-Data-Protection-Laws.pdf (Last modified April 09, 2023)

- **Right Based approach:** Cross-border data flows are subject to stringent compliance obligations as a result of the Right Based approach. This regulatory strategy, which sits in the middle of the pack, often includes conditional transfer restrictions. The main proponent of this strategy is the EU. [16]

Data Localisation Laws in India: In India data Localisation Laws are scattered through various provisions in different acts in different fields

- Section 4 of the Public Records Act of 1993 prohibits any transfer of "public records" outside of India.[17]
- Telecom Service Provider Unified Access Licence, 2004 requires local processing and storage of subscriber information, and it forbids the transfer of user and subscriber-related accounting information.
- The Information Technology (IT) Act of 2000 and the Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011 prohibits the transfer of sensitive personal information by a body corporate unless the foreign counterpart can provide the same level of data protection as required by the IT Rules.[18]
- The Companies (Accounts) Rules of 2014 and the (Indian) Companies Act of 2013: In accordance with Sections 88 and 92 of the Companies Act, the covered organisations are mandated to keep the financial records at the company's registered office.
- The MeghRaj Initiative, 2014 (an Indian government initiative on the data storage practises of government departments and authorities), mandates that any cloud service providers with whom it has contracted must keep "the data centre facilities and the physical and virtual hardware" exclusively in India.
- According to paragraph 3(9) of the Insurance Regulatory and Development Authority of India {IRDAI} (Maintenance of Insurance Records) Regulation, 2015, covered organisations must maintain insurance data domestically.[19]
- According to the 2015 National Telecom MDM Roadmap, all M2M gateways and application servers "servicing customers in India must be physically located in India."[20]
- All FDI-receiving firms in the broadcasting industry are required by the FDI Policy 2017 to ensure that subscriber data is processed and stored locally. The movement of subscriber data outside of India is likewise prohibited.[21]

[16]Avaialble at https://globaljournals.org/GJHSS_Volume21/2-Data-Protection-Laws.pdf (Last modified April 09, 2023)
[17]"The Public Records Act, 1993," National Archives of India, 1993, http://nationalarchives.nic.in/content/public-records-act-1993-0.
[18]"The Information Technology (IT) Act, 2000," Indian Ministry of Electronics and Information Technology, 2000, https://www.meity.gov.in/content/information-technology-act-2000.
[19]"IRDAI (Outsourcing of Activities by Indian Insurers) Regulations," Insurance Regulatory and Development Authority, 2017, https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1.
[20]"National Telecom M2M Roadmap," Indian Ministry of Communications and Information Technology Department of Telecommunications, May 2015, https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf.

- ❖ According to paragraph 2(i) of the Reserve Bank of India's Directive 2017-18/153, which was issued under the Payment and Settlement Systems Act 2007 on April 6, 2018, covered organisations must retain payment data within India.[22]
- ❖ Data localisation was suggested by the Justice Srikrishna Committee in its report's 2018 Draft Personal Data Protection Bill. With increasing levels of restrictions on the flow of personal data, sensitive personal data, and critical personal data, respectively, it established a cross-sectoral data localisation need[23]. In the 2019 Personal Data Protection Bill, was introduced in the Indian parliament, but failed to become the law in August 2022.
- ❖ **Digital Personal Data Protection Bill 2022:**The Ministry of Electronics and Information Technology ('MeitY') recently released the (long-awaited) draft Digital Personal Data Protection Bill, 2022 ('DPDP Bill'), and this new Bill will be introduced in the Monsoon Session of the Parliament in July in an effort to establish a comprehensive data protection regime in India.

According to Sec.17 of the DPDP Bill, 2022, the Central Government is required to inform nations or territories outside of India to which a data fiduciary may transfer personal data. The provision further indicates that the government will later notify the public of the terms and conditions under which such a transfer will be permitted. However the DPDP Bill has failed to provide a limit for the various factors that might be taken into account when notifying such nations. [24]

According to Section 18 of the draft Bill, cross-border personal data transfers are allowed on the following conditions:

- When processing personal data is required to uphold a legal right or claim;
- Processing is done for the purpose of preventing, detecting, looking into, or prosecuting any crime or law violation;
- Processing is required for the execution of judicial and quasi-judicial tasks in India by any court, tribunal, or other entity;
- The processing of the personal data is done outside of India in accordance with an agreement that any person headquartered in India has with any person outside of India.

According to the New Draft Bill Transfers of personal data outside India will occur to nations that have been notified by the Indian government. These nations will be chosen

[21]"Consolidated FDI Policy," Indian Ministry of Commerce and Industry Department of Industrial Policy and Promotion, August 28, 2017, https://dipp.gov.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17_1.pdf.
[22]Reserve Bank of India, "Storage of Payment System Data." Also see paragraph 6.4.9 of the "Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs)" Reserve Bank of India, 2020, 34 https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=3864.
[23]Srikrishna Committee of Experts, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, 88.
[24] Available at https://www.ahlawatassociates.com/blog/analysis-of-digital-personal-data-protection-bill-2022/?utm_source=mondaq&utm_medium=syndication&utm_term=Privacy&utm_content=articleoriginal&utm_campaign=article (Last modified March28, 2023)

after taking into account all relevant factors. Previous definitions and guidelines for transferring sensitive and critical personal data across borders have been eliminated. The recent privacy bill attempts to strike a balance by allowing cross-border data flows to "preferred geographies" (which are not defined in the bill) as announced by the Central Government, but it will never be certain which countries will continue to be a preferred geography in the near or distant future.The new bill is still being debated, but it may very well serve as a launchpad for the nation's digital engine to accelerate with the required trails in place to protect sensitive and personal data of citizens.[25]

Data localization may reduce a nation's reliance on MLATs (Mutual Legal Assistance Treaties). These are ratified to make it easier for two countries to exchange information. India has ratified to MLAT's with 45 countries.[26]

Risks involved inData Localisation: The critics however suggest that the process of Data Localisation may have the followingrisks

- Politically and diplomatically, localization may have an effect on India's commercial relations with its allies.
- Security Threats: The physical vulnerability to exploitation by anyone physically obtaining the data or gaining remote access to the data is inevitably increased by storing the data across numerous physical locations. Therefore, the infrastructure needs to be supported by reliable security measures, which involves significant cost.
- Economic impact: By raising compliance costs and entrance obstacles for foreign service providers and limiting investment or shifting these costs to consumers, restrictions on cross-border data flow could impair overall economic growth. The high expense of establishing a data centre in India along with the unsuitable weather are the main compliance issues. Furthermore, reciprocal limits imposed by other nations may prevent access to the data in a number of other jurisdictions, which might be problematic for start-ups aiming for worldwide prominence.

Data Localisationin various countries: Various countries in the world have adopted Data Localisation measures in the following manner

Russia: One of the first and strictest broader perspective data localisation rules in the world was implemented in Russia. Federal Law No. 242-FZ, which governs data localization, was enacted on September 1, 2015.[27] It establishes a general rule requiring that any data gathered from Russian residents be handled and maintained on Russian soil. The location of the storage facility must be in accordance with the nation's privacy laws and must be reported to

[25] Available at https://www.business-standard.com/article/current-affairs/personal-data-all-you-need-to-know-about-data-localisation-rules-in-india-123010600429_1.html (Last modified April 01,2023)
[26] Ibid
[27]Matthias Bauer, Martina F. Farracane & Erik van der Marel, Global Commission on Internet Governance,Tracing the Economic Impact ofRegulations on the Free Flow of Data and Data Localization (May 2016),https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf (Lat modified April 08, 2023)

the authorities. Roskomnadzor, Russia's data protection and telecommunications agency, is in charge of such enforcement.[28]

Kazakhstan: Since 2005, laws governing data localisation have been in effect in Kazakhstan, where websites using the.kz domain are required to keep all of their data locally. Kazakhstan has adopted a strict method of data localisation, following Russia's lead. Additionally, they have a rule requiring the local keeping of data gathered from nation residents[29]. Data Protection is the main motivation behind such a defensive approach to cross-border data exchanges.

China: Chinese follow a very strict Data Localisation regime. None of their data is stored without passing a security review. All personal and important data has to be stored within the territory of China.[30]

Nigeria: Nigeria has sector-specific data localisation. Subscriber data and customer data must be stored locally for cyber security concerns, according to National Information Technology Development Agency (NITDA) Guidelines for Nigerian Content Development in Information Communication Technology[31]

Vietnam: The Vietnam Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72, revised in 2013) requires domestic and foreign providers of Internet-based services to maintain at least one server within the country's territorial jurisdiction and make those servers accessible for inspection by the government upon request[32]. Vietnam also enforces regulations on businesses that deal in commercial encryption goods, requiring them to obtain licences and follow local data storage laws.[33]Vietnam included these rules in its law enforcement and cyber security measures.[34]

Indonesia: Around 2012, Indonesia started enacting rules and regulations pertaining to data localisation. Electronic System Providers (ESPs) operating systems linked to "public services" are required by Guideline 82 to keep and use data about Indonesian people there. Many Electronic System Providers (ESPs), including government agencies and companies with only a digital presence in Indonesia that collect personal data about citizens there, are now subject to the data localisation regulations due to the expansive definition of public services. Definition of "personal data" and more detailed explanations of Indonesia's data handling requirements at each stage of the lifecycle of an individual's data are provided in

[28]Bret Cohen, B. H. &. C. W., 2017. Data Localization Laws and Their Impact on Privacy, Data Security and theGlobal Economy. Antitrust, 32(Fall), p. 107.
[29]Daniyar Sabitov, Information Security in Kazakhstan: Protection of Data and Ideas (Inst. of World Econ. & Politics Working Paper, Mar. 2016),
[30]Ibid
[31]Office for Nigerian Content Dev. in Info. & Commc'n Tech., Guidelines for Nigerian Content Development inInformation Communication Technology 12.1(4) and 14.1(2), at 19, 23
[32]Decree No. 72/2013/ND-CP of July 15, 2013 On the Management, Provision and Use of Internet Services and Online Information,
[33] Law No.: 86/2015/QH13, Law on Network Information Security, arts. 10(3) and 31(1),
[34] Anupam Chander &; Uyen P. Le, Data Nationalism, 64 EMORY L.J. 677, 706 (2015

Guideline 20, an implementing guideline of Indonesia's Electronic Information and Transactions Law and Regulation 82, which became effective in December 2018.[35]

Choice-based approachin United States of America:Data localisation is approached in two ways in the US. Even though the US does not have an express right to privacy, they adhere to strong data localization standards when the government processes personal data. However, as recognised by US courts, the First, Fourth, Fifth, and Fourteenth Amendments of the US Constitution collectively grant a Fundamental Right to Privacy. Different regulations safeguard privacy in relation to the protection of data belonging to US individuals. Data protection laws exist in some states. In order to localise data processing for the commercial sector, the US adopted a choice-based approach.[36]

Right-based approach in European Union:The General Data Protection Regulation of the European Union regulates data localization in a right-based approach. Every person has the fundamental right to privacy, which has been incorporated into the concept of human dignity. The right to privacy is acknowledged in Article 7 of the European Charter of Fundamental Rights, and the right to the protection of personal data is mentioned in Article 8. The EU drafted a consistent data protection law based on the rights that people have, which will guarantee data protection and cross-border data flow among EU countries.To guarantee the people their right to the protection of their personal data, GDPR governs data at two levels,firstly during the collection and secondly processing of that data as well as after it has been processed. The majority of circumstances include limitations on the gathering of sensitive personal information, including information about racial or ethnic origin, political ideas, religious or philosophical beliefs, trade union membership, and sexual orientation and health data. Therefore, processing personal data legitimately requires adhering to a wide range of standards and guidelines, such as purpose specification, data minimization, data quality, security precautions, etc.[37]

Conclusion and Suggestion: The achievement of Data localization related norms depends on broad policy level thoughts. This could entail revising Mutual Legal Assistance Agreements, amending various Surveillance Laws, promoting the creation of adequate digital Infrastructure, and creating appropriate data-sharing laws that respect the rights of third parties and permit the use of data for socially beneficial purposes.The authors also have tried to highlight some of the risks involved in the process of Data Localisation which needs to be worked on.A localization architecture that includes both local data storage and worldwide processing appears to be the greatest choice for promoting greater economic growth in India.Since everyone who uses the internet sends data in some way or another, the requirement for data localization strengthens the safety of personal data. Considering all the

[35]Gilang Ardana, KOMINFO Releases Personal Data Protection Regulation, Am. Chamber of Commerce in Indonesia (Jan. 17, 2017),
[36]Framework, T. C. O. E. O. A. D. P., 2017. White Paper of The Committee Of Experts On A Data Protection Framework For India.New Delhi: Ministry of Electronics and Information Technology (MeitY).
[37]Framework, T. C. O. E. O. A. D. P., 2017. White Paper of The Committee Of Experts On A Data Protection Framework For India.New Delhi: Ministry of Electronics and Information Technology (MeitY).

above factors and existing legislations focussing on Data Localisation it becomes imperative for a booming economy like India to frame a comprehensive law which mandates Data Localisation. To balance the differences and trade-offs between various localisation schemes, policymakers will have to work towards achieving this goal. As a significant contribution to ongoing policy discussions concerning the benefits and risks of various localization strategies, this paper attempts to provide an explanation of these findings.We believe that this article will be a helpful frame of reference for academics and policymakers who are striving to address some of the key issues in the data localization debate.