

India's Data Localization Journey:

Privacy, Security, and Beyond

Abstract: Data localization has become a hot topic in India in recent years. The Indian government has been taking steps to mandate the storage of certain types of data within India's borders, citing concerns about privacy, security, and sovereignty. However, this move has also raised concerns about increased costs, reduced efficiency, and potential barriers to trade. This article provides a comprehensive overview of data localization in India, examining the concept from all angles. We have discussed the reasons behind the government's push for data localization and the types of data that are affected. We also explored the impact of data localization on various industries, including technology, finance, and e-commerce. Additionally, we analyzed the legal and regulatory framework surrounding data localization in India, including the relevant laws and guidelines, as well as the implications for businesses operating in India. Finally, we have considered the international perspective, looking at how data localization fits into the global data governance landscape and the potential impact on India's relationships with other countries. Overall, this article aims to provide a 360-degree view of data localization in India, helping readers to understand the motivations, challenges, and implications of this contentious issue. The article explores the concept of data localization and its impact on data flow and privacy protection. It provides a comprehensive review of the issues faced by India in terms of data protection and localization, including the impact on emerging technologies such as cloud computing, E-commerce, big data, artificial intelligence (AI), and the internet of things. The article also discusses the legal and regulatory framework surrounding data localization in India and compares it to other nations. It suggests that India should develop policy initiatives to encourage transparent and clear international standards on data security, as well as enabling higher levels of digital innovation in developing countries. The article presents a balanced view of the pros and cons of data localization and provides recommendations for addressing the issue.

Keywords: Data localization, jurisdiction, Artificial Intelligence, data privacy.

1. Introduction

Data localization become a contentious issue in these past years, particularly in India, where the government has been taking steps to mandate the storage of certain types of data within its borders. The aim is to enhance privacy, security, and sovereignty, but this move has also raised concerns about increased costs, reduced efficiency, and potential barriers to trade. In this article, we explore the concept of data localization and its impact on data flow and privacy protection. We provided a comprehensive review of the issues faced by India, including the impact on emerging technologies such as cloud computing, e-commerce, data, AI, & and the Internet of things. We **have** also **discussed** the legal and regulatory framework **of** surrounding data **localized** in India **and** **compared** it to other nations. Additionally, we suggest that India should develop policy initiatives to enhance transparent clear international levels of data security, as well as **enable a** higher degree of digital innovation in all developing countries. We **have presented** a balanced view of the pros and cons of data localization and **provided** recommendations for addressing the issue.

In today's digital age, personal data has become an essential commodity. We often share our personal information with various service providers, such as social media platforms, e-commerce websites, and financial institutions, either willingly or unwillingly. However, the increasing number of cybercrimes and data breaches has made us question whether our personal information is safe or not. In India, where there is no proper legal framework for data protection and privacy, the fear of sharing personal information can be even more daunting. While the Indian Information Technology Act 2000 has certain provisions related to the collection, use, and protection of personal information, it is not enough to ensure adequate data protection. The lack of a robust data protection framework has made India vulnerable to cyber-attacks and data breaches, which can have severe consequences for individuals and businesses. Therefore, it is essential to establish a strong legal and regulatory framework to safeguard personal data and privacy in India.

The concern over data privacy and protection is not just limited to India but is a global issue. With the increasing digitization of the world, personal data has become a valuable commodity that can be exploited for financial gain. This has led to the emergence of data localization laws, which require that data be stored and processed within a specific jurisdiction, either exclusively or non-exclusively. These laws are often seen as a non-tariff barrier to trade and are viewed as hindering the growth of trade in a digital world [2].

In India, information localization laws have gotten to be a fervently talked about subject. The government has presented a few measures aimed at ensuring information and advancing nearby information capacities, such as the Information Assurance Charge 2018 and the Information National E-commerce Arrangement. Be that as it may, there are concerns over the effect of these measures on developing innovations such as cloud computing, e-commerce, huge information, AI, and the web of things [4]. The Indian Data Innovation Act 2000 has certain arrangements related to individual data, but there are still crevices within the legal system that ought to be tended to. In such a situation, sharing individual data can be a cause for fear and doubt, especially in cases where the information is being shared automatically. This article aims to deliver a comprehensive audit of information localization and its effect on information stream and security assurance, with a particular center on India. It presents an adjusted see of the stars and cons of information localization, examines the legitimate and administrative system encompassing information localization in India, and gives suggestions for tending to the issue. The article proposes that India ought to create approach activities to empower straightforward and clear worldwide measures on information security, as well as empowering higher levels of computerized advancement in creating nations [5].

The right to privacy as per Article 21 has been a fascinating development in the Indian constitutional Jurisprudence given by the Supreme Court. Many of us may find it irrelevant and even give a thought to

how does right to privacy concerns data localization or data protection.

According to Black's Law Dictionary, various scholars and legal experts in different ways have defined the concept of privacy. Black's Law Dictionary defines privacy as the "right to be let alone" and further elaborates it as the right of an individual to be free from any unwarranted publicity, by the public in matters that are personal and do not concern the public at large. In essence, privacy is the right of any person to maintain control over their personal information and to decide who has access to it. It includes the right to keep personal matters confidential and to be free from undesirable interruption or observation. Security may be a crucial human right that's recognized by numerous universal and national laws, including the Widespread Announcement of Human Rights and the International Pledge on Respectful and Political Rights. In India, an incomparable court in a point of interest judgment announced the correct to security as an essential right in 2017. The court recognized that security is essential for the nobility and independence of a person and is an inborn portion of the correct to life and individual freedom ensured by Article 21 of the constitution [6].

Despite the acknowledgment of security as a crucial right, there are still numerous challenges in ensuring it, particularly within the advanced age where individual data is continually being shared and collected. The need for an appropriate legitimate system for information security and protection in India makes it more troublesome to defend individual data. Therefore, it is vital for people to be mindful of their protection rights and take fundamental safeguards to ensure their personal data [7]. As there's a persistent up-gradation the ought to pigeonhole protection as a crucial right in India has ended up fundamental. The correct to protection has been as of late recognized as an essential

right rising essentially from Article 21 of the Structure, In Equity K.S. Puttaswamy (Retd.) vs Union of India (Equity K.S. puttaswamy vs Union of India, 2017) Enterprises are frequently coming up with the modern thought of collecting, handling managing with the individual data of a person. The fast development within the field of digitization of India's financial framework has driven organizations and specialists to understand that information plays a vital part in the improvement of the economy. Even the progressed economy of created nations just as the European Union and the United States of America have considered information as the root of economic advancement and have executed unused enactment to ensure and preserve touchy information. Within the case of Equity K.S. Puttaswamy vs Union of India in 2017, the Preeminent Court of India recognized the significance of information security and protection within the advanced age. The court acknowledged that enterprises and specialists are continually collecting and handling individual data, which this information plays a crucial part in the development of the economy. The court is moreover famous that progressed economies such as the European Union and the Joined together States have executed enactment to ensure touchy information, which India ought to take after suit. The court recognized that the need for a legitimate lawful system for information security in India has driven concerns over protection and the security of individual data. The court's choice within the Puttaswamy case was driven by the sanctioning of the Individual Information Assurance Charge in India in 2019. The charge points to secure the security of people by directing the collection, preparation, capacity, and utilization of individual information by enterprises and specialists. The charge moreover gives for the foundation of an Information Security Specialist to supervise and enforce data assurance laws within the country. Overall, the choice within the Puttaswamy case highlights the require for solid data protection laws in India to ensure individuals' security and individual data within the computerized age.

The display laws related to information security in India come beneath the Data Innovation Act (IT Act) 2000, and the rules surrounded there beneath, the Indian Correctional Code (IPC)1860, other sectoral directions. In showing disdain toward their presence, India does not serve laws and controls concurring with the energetic circumstance. To overcome this circumstance, the Service of Gadgets and Data Innovation (Meity), Government of India (GOI) built up a committee of specialists beneath the chairmanship of the previous Preeminent Court judge Equity BN Srikrishna.

The most errand of the committee was to pinpoint the slip within the display information assurance direction and to put together information security laws that were vigorous and comprehensive and draft the Individual Information Security Charge (PDP) which is however to be sanctioned. in line with the changing mechanical scene and worldwide benchmarks. The committee submitted a draft Individual Information Security Charge, 2018 (PDPB) in July 2018, which proposed a system for ensuring the security of people and controlling the handling of individual information in India.

The PDPB proposes a few key changes, such as growing the definition of individual information, presenting modern categories of delicate individual information, making commitments for information

fiduciaries and processors, and building up an Information Security Specialist of India (DPAI) to direct and uphold information assurance laws. The charge also proposes exacting punishments for non-compliance with information security controls, counting fines and detainment. Be that as it may, the PDPB has not however been passed into law, and India right now does not have a comprehensive information assurance system. As a result, there are concerns over the security of individual information in India, particularly given the country's quickly developing advanced economy and the expanding utilization of information by enterprises and government substances [8].

Over the period, the Government of India has been attempting to adjust to the transformative potential of the advanced economy. Their activity towards Information localization and cross-border information transmission shows that information could be a collective asset and national resource, over which citizens have a majestic right and information requires certain restrictions to be set input. This has primarily been worn out to hone constraining information capacity and prepare information for particular geographies. The report submitted by the Srikrishna committee was almost information assurance issues confronted by India. It too demonstrated that the biggest protest of the Government of India was to open the information economy while keeping the information of the citizens secure and secured.

1.1 Motivation:

The issue of data localization has gained significant attention in recent years, particularly in India. There have been numerous debates, discussions, and policies formulated around this topic. However, despite the growing importance of this issue, there is a lack of comprehensive literature that provides a 360° view of data localization in India. As a result, there is a need for a review paper that brings together various perspectives and provides a holistic understanding of the issue. This paper aims to fill this gap by presenting a comprehensive review of the literature on data localization in India, from various angles.

1.2 Problem statement:

Data localization has become a critical issue in India due to various reasons, such as national security, data privacy, and data sovereignty. However, the lack of a comprehensive understanding of the issue and the absence of clear guidelines have resulted in a fragmented approach towards data localization. Moreover, there is a lack of consensus among various stakeholders, such as policymakers, businesses, and civil society, on the benefits and drawbacks of data localization. This review paper aims to address these issues by providing a 360° view of data localization in India, analyzing the various perspectives, and highlighting the challenges and opportunities associated with it. By doing so, the paper aims to provide a clear understanding of data localization in India and its implications for various stakeholders.

The major contributions of the review paper "Data Localization in India – A 360° view" are:

- A comprehensive understanding of the concept of data localization, including its definition, rationale, and objectives. The paper provides a detailed analysis of the various types of data localization policies adopted by different countries, highlighting their benefits and drawbacks.
- A review of the literature on data localization in India, covering various aspects such as data protection, national security, economic implications, and legal challenges. The paper presents an analysis of the existing data localization policies in India and their impact on various stakeholders.
- An overview of the stakeholder perspectives on data localization in India, including the views of policymakers, businesses, civil society organizations, and international organizations. The paper examines the divergent views and provides a nuanced understanding of the debate around data localization in India.
- An assessment of the challenges and opportunities associated with data localization in India. The paper identifies the major challenges faced by businesses and policymakers in implementing data localization policies and highlights the potential opportunities that data localization can create for India.
- A set of recommendations for policymakers and businesses on how to navigate the challenges associated with data localization in India. The paper provides guidance on how to design and implement data localization policies that balance the competing interests of various stakeholders and create a conducive environment for businesses to operate in India.

2. Sri Krishna Committee report

This report was based on a principal brief, shared by the entire committee that if India is planning to form itself within the computerized economy scene of the 21st Century, it ought to have an appropriate legitimate system relating to the individual information that can work as a resource for the creating world. Keeping up such a conviction that the security of individual information can hold the key to strengthening, advance, and development. Beneath this Committee's draft, the 'right to be overlooked, is characterized in an unexpected way – the correct to confine or prevent the continuing revelation of individual information. The right to security has been recognized as a principal right in point of interest judgment passed by the preeminent court within the case of Equity K.S. Puttaswamy (Retd.) v. Union of India⁴ on 24th Admirable 2017, the seat consistently recognized a principal right to protection of each person ensured by the structure, inside article 21 in specific and portion III on the total. The choice of M.P Sharma and Kharak Singh was overruled.

Some key Suggestions made by the committee-

- Personal information collected, shared, uncovered, or something else handled by the companies acclimatize beneath Indian Law. Be that as it may, the information security law may engage the central government to avoid such companies which as it were prepare the individual information of outside countries not shown in India.
- Sensitive individual information counting watchword, money-related information, wellbeing information, sex life, sexual introduction, biometric and hereditary information, and information that uncovers transgender status, intersex status, caste, tribe, religion, or political conviction or affiliations of people. In any case, the DPA will be given the residuary control to inform advance categories in understanding with criteria set by the law.

- Personal information might be prepared as it were for the reason that's clear, particular, and legal
- Every person will be given a right to pull back the assent **given under** Article 21 of the Indian constitution
- All firms ought to designate **an** information assurance officer. Moreover guaranteeing at **least** one duplicate of individual information to be put away in India.
- Section 47 of Individual Information Security Charge, **2018** Exceptions have been given for the preparing of individual information for writer purposes, or for **an absolutely** individual or household purpose.
- Penalties run from 2-4% of a company's around-the-world turnover or fines between Rs. 5 crore and Rs. 15 Crore whichever is higher.
- The law will not have retrospective application and **it'll** will come into drive in **an organized** and phased manner. Existing acts such as the Correct to Data, Aadhaar, and Data Innovation Act will need to be amended.

The proposal specified by the committee on major or burning issues such as assent, setting up an information specialist, the definition of individual information, and touchy individual information at the side information localization was escalation anticipated for their suggestions on tech majors such as Google, Facebook, and Twitter among other.

The report in detail **also** notices the existing approach for information security which created countries are taking after. The three approaches mainly taken by the nations are the US, EU, and China. Firstly, the US **follows a Laissez- fair** approach and does not have an overarching information assurance system. They have the entire recognized right to security by piecing together the restricted protection assurance reflected within the, to begin with, fourth, fifth, and fourteenth **revisions** to the US Constitution.

EU, information security is established on the got to maintain individuals' respect. Central to nobility is the privacy of the people by which the people have the correct to choose whom ought to

they share the information. China outlines its garden with the intrigued collective center, based on its claim privileging The collective over the individuals.

The conceptualism of the state of the structure is based on two boards. Firstly, the state may be a facilitator of human advance. Subsequently being commanded by the structure in portion four Mandate Standards of State Arrangement (DPSP) to serve the common great. Besides, the state is inclined to abundance. **Consequently**, it is checked by both a vertical (government structure) and even (three organs of government) division of control, as well as exploring each person with the basic rights that can be implemented against the state.

Every change presented is to move forward lives in India by clearing the way through **a computerized** economy. Each change has its claim **effect** it can be positive as well as negative. **These small changes can prevent a bigger disaster.**

The past confirmation by Facebook on Cambridge Expository Trick (2018), the trick took put in Walk 2018, it started the awesome protection arousing. The Unused York Times working with the perception of London and the **Gatekeeper, got** a cache of archives from interior Cambridge Expository, the information firm basically possessed by the right-wing benefactor Robert Mercer 5. Information of numerous clients **was** spilled for the reason of Trump's decision. It was found through the report that the workers of Cambridge Explanatory were enthusiastic **about offering** mental profiles of American voters to political campaigns, getting the private Facebook information of 87 million clients – the biggest known spill in Facebook history. Among these 5 lakhs were Indian clients. After, the occurrence Facebook **has chosen** to execute the EU's Common Information Assurance in all regions of operation not fair within the EU.

The latter, Dominos Information Breach where individual data such as title, address, exchange, and other points of interest of over 18 Crore orders was spilled. This information breach was to begin brought in by Web Security Analyst Rajshekhar Rajagharia counting **130TB of employee data** files and customer details. The scariest portion of this information breach was that individuals may utilize this information for spying on distinctive individuals. By **looking at anyone's** versatile number, **a person's** past area with date and time. One of the security specialists Prakash Chime, Head of **a client** victory and SE lead, India and SAARC, checkpoint computer program Mechanical said on the leak "Organisation taking care of end-user-end ought to be contributing more in cybersecurity arrangements and hone that will improve their security posters"

Air India Breach, the occurrence took put in February 2021. It led to the breach of information of around 4.5 million travelers due to the cyberattack on the airline.

Air India reacted: "This is to advise that SITA PSS, our information processor of the traveler benefit framework (which is capable of putting away and preparing of individual data of the travelers) had as of

late been subjected to a cybersecurity assault driving to individual information spill of certain travelers. This occurrence influenced around 45 lakh information subjects within the world. While we had gotten the primary notice in this respect from our information processor on February 25, 2021, we would like to clarify that the personality of the influenced information subjects was as it was given to us by our information processor.

The other major cyber occurrence in the later past incorporates easyJet (EZJ.L) which final year said programmers had gotten to the mail and travel points of interest of around 9 million customers.

UNDER PEER REVIEW

3. Article 29 of the Law on the Protection of Personal Data No., Protection of Personal Data, “Personal data refers to data relating to or relating to a person whose identity can be determined directly or indirectly, including any characteristics, qualities, qualities or other. These attributes are the identity of a semi-real person a relationship component of attributes or a combination of attributes and other information. (Meity), **The government** of India is one step closer to enacting Indian data privacy laws.

In December 2019, the Minister of Electronics and Information Technologies of India introduced the new Personal Data Protection Bill ("Draft") in the Lok Sabha, the lower house of the Indian Parliament. The bill was sent to an elected committee made up of members of the Executive Board and Executive Committee. The updated bill retains the core structure of the previous 2018 draft, following the model provided by the GDPR (General Data Protection Regulation). However, the 2019 bill brought some important changes, including some controversial issues from the 2018 bill, such as necessary territorial information and some regulations regarding criminal sanctions. The 2019 draft contains some provisions that were not included in the 2018 draft, such as the development of the law.

Deletion, obligations related to anonymous data, and some special requirements for social media such as Twitter, Facebook, and Instagram.

In the Personal Data Protection Law of 2018, the Data Protection Authority has one director and six full-time members, while in the 2019 Law, the Data Protection Authority has less than six members. Unlike the 2018 Act, DPA does not create new categories of sensitive personal data.

4. The motivation behind the Privacy Law No.

The right to privacy is an important right, emphasizing that personal information should be protected as an important part of private information. **The development of the digital economy has increased communication between people. Everyone needs to feel comfortable after sharing personal information. Therefore, in order to gain trust and maintain interpersonal relations, it is necessary to establish regulations that protect the freedom of individuals over their personal data and inform them about the flow and use of personal data. Providers and processors of information inform them of their rights against persons whose personal information is processed, provide appropriate procedures for the use of organizations and measures for the processing of personal data, and determine border crossing rules.** To transfer personal data and to ensure that the responsibility of the institutions that process personal data is maintained, to ensure that unauthorized errors and damages are corrected, and to monitor activities managed in favor of data protection authorities.

In 2019, most of the bill (2018 Bill) submitted by the Srikrishna Justice Council is still in effect. **However** 2019 introduced a new concept different from some aspects of the 2018 Act. Key differences include: but the need for data space remains for important and important personal data - The law governs some kind of

mode. Minimize local data and data transfer coverage by following these guidelines for sensitive and important personal data. Basically, the Law imposes three burdens:

Personal Data - Under the Law, no local or data transfer restrictions apply to excluded personal data that is "sensitive" or "critical". This personal data may be located outside of India and no transfer restrictions apply.

Special Categories of Personal Data - The Law on Special Categories of Personal Data largely reflects the 2018 draft. According to the law, "sensitive personal data may be transferred outside of India, but personal data will be stored in India.

At the same time, the bill announced strict contractual procedures to facilitate the transfer, and in many cases, trustees must obtain "consent" to use the listed procedures. Sensitive personal data includes a variety of "specific personal data" under the GDPR - data related to health, religion, sex life, political beliefs, and biometric and genetic data - but unlike GDPR, financial data is intended. Specifically, the password has been removed from the invoice context.

Sensitive Personal Data - As the Bill was drafted in 2018, the Law allows the government to define certain personal data as sensitive data. There is no mention of any limits on the powers of the government, and such coercion cannot be exercised outside India.

While the law will provide for strict territorial regulations for entities that continue to transpose or are deemed to provide adequate protection (and the security or interests of the country will not be affected) or some significant protection. Create a special interest.

2. The Law of 2019 introduces the concept of "data controller consent" through data processing, which can control the authorized use of rights such as data portability, right to rectification, and right to be forgotten, under the Data Protection Law 2019.

3. Personal Data Act 2018, DPA cannot list new names of Personal information, it is protected under the Data Protection Act 2019. This authority is given only to the central government.

4. The Law of 2019 allows the central government to direct the data custodian/data processor to provide non-personal information (also known as non-personal data) to provide quality services again or to create legal documents.

5. Data Protection Law 2019, Facebook, Twitter Instagram, etc. social media self-identification should be allowed, in other words, the bill would require social media to "allow users who sign up for their services from India or use their services in India to ensure that their income is as stated or recorded". Granted funds

must receive "visible and verifiable certificates". The law also allows the government to allow media outlets to process "sensitive information" in consultation with the DPA (Data Protection Act, 1998). With significant dilution of Law No. 2018, childcare centers will be excluded from the Law's limited rights and only limited space and problem

- (i) The formation process of Law
- (ii) Priority
- (iii) Dimension.

5. Data National E-Commerce Act

The Government of India issued the National E-Commerce Act in 2019, which issued a legislative act to restrict cross-border data. There is also a business to collect or process sensitive information locally and store it abroad. Over the last few years, e-commerce has continued to grow and the importance of business in the digital space has increased all over the world and in India. This digitalization has created job opportunities for those who deserve it.

E-commerce in India, as in the rest of the world, has been growing steadily in recent years. The e-commerce company recently reported \$4 in sales.

October 2020 festival week (October 15-21), crossing 1 billion across the platform, taking 55% share from Tier 2 cities such as Asansol, Dhanbad, Ludhiana and Rajkot due to the increasing demand for smartphones.

The draft of the e-commerce policy says about the holistic policy. A holistic policy that will try to look at aspects for a long time we have been wondering where there be a regulator when it comes to e-commerce companies. The government now seems to be proposing how it will monitor e-commerce companies like Amazon, Flipkart, Myntra, Ajo, etc.

The draft policy identifies the cross-cutting tendency of e-commerce and the existence of laws and regulations. Therefore, investigative authorities "must ensure that swift action is not affected by areas of law."

The different laws currently governing e-commerce include income law, consumer protection law, IT law, competition law, payment and. The law deals with the laws related to contracts, companies and GST.

Some of the highlights of the draft e-commerce policies are-

- It is Mandatory to register with the identified authority by the government.
- The government may collect the information data from the e-commerce platforms to aid in the making right decision.
- The actual monitoring will be done by the standing group of Secretaries who will give from time to time recommendations to address policy-changing
- Standing group of Secretaries will play a major role in administering the e-commerce policy

In this way, e-commerce players domestic as well as global small or large will be monitored.

2. Level playing field

- One of the regulatory challenges that have been identified with the government is to have a level playing field where it conveys how e-commerce can lead to one or two dominant players and it wants to bust the monopoly that exists. The act can create a mechanism in holistically inquiring into the violation of laws. The government may be powered to create a mechanism and from time to time it can see if any laws are being violated and decide action thereafter.
- There is a tendency for 1 & 2 companies to exercise and control regarding the repository data collected.

- Entities that have the maximum info regarding their can dominate This can lead to the subvention of competition

3. Handling of data

- We have been told that the draft of the e-commerce policy proposes the cross-border flow of data of Indians and their transaction should not be permitted. No cross-border flow of data
- The Indian firm will have to audit an e-commerce company's data. This could turn into beavery contagious clause

4. Inclusive growth

- Streamlining regulatory processes to ease the burden of compliance
- Long-term goal to make GEM a marketplace place ordinary consumers to buy
- State government transform emporiums to go online to have-emporiums

5. Enhancing export

This is something that the government is very committed to

- It wants to digitally, integrate multiple interfaces. CBIIC, GSTN, DGFT, and Dept of Posts
- India post to build specialized, low-cost tractable solutions for e-commerce exporters
- Strengthen Foreign Post Office to become delivery hubs

6. Fair competition

- The government wants to ensure that equal treatment should be given to sellers/vendors

- The e-commerce company should have an algorithm that must not prioritize vendors, sellers
- There must be a clear and transparent discount policy

7. Free and informed choice

- Use of an algorithm that is not biased
- Services consumer must match the description on the platforms
- Consumers the country of origin, valued in India

8. Anti-counterfeit and anti-privacy

- Liability shall be joint of e-commerce entity and sellers
- Must expeditiously handle consumer counterfeit issue
- Industry stakeholder body to identify rogue e-commerce entities.

6. Data Localisation: Pros and Cons

As with the invention of the internet, information can flow freely around the world without restrictions. Although some countries in the world, such as China, are not interested in this information, Russia is trying to control the information in the region. India passed the Privacy Act (2018) bill, so every Indian citizen should know all the pros and cons of local documents before this bill becomes a real Law.

Pros of Data Localization–

1. It will secure the data of every citizen of India and provide data privacy & and data sovereignty from foreign surveillance. It is the right of people to secure their own data.
2. It will secure national security by accessing the data that is localized by the Government as currently, Indian Law Enforcement agencies rely on Mutual Legal Assistance Treaties (MLAT). It will become easy for the MLAT to access the data.

3. It will minimize the conflict of jurisdiction because of the cross borders' data sharing & most importantly delay in justice given in the case of the data breach.

4. The most optimistic approach toward data localization is Corporatism. Data is precious it can be an important factor if it is properly analyzed.

5. Data Localization is very much useful in controlling **crime** if there is money fraud during the investigation of the crimes there is a need for payment information and if this particular data is stored overseas it will be great difficult or it will take lots of time to obtain the permission from granting access of data. This will delay in solving the crimes and it can be solved by storing the data within the country.

6. Data Localization will benefit the government in the **form of Tax** as data can be considered as a national resource so the nation's Government has the right to produce income from that source. Data in and out should be taxed the same as the inflow and outflow of goods.

7. As our nation has a lack of employment and the data localization laws provide several data centers. It will create employment that will boost the economy of India.

Cons of Data Localization–

1. The freedom of the Internet will be snatched by the Data Localization Law. The Internet is solely based on the free flow of data and if Government imposes a tax on this free flow of data, the Internet will be destroyed.

2. India's decision on Data Localization will be not a prudent decision as India doesn't have a system to ensure data protection. As the country that is planning for data Localization has an integrated system, India should not rush toward Data Localization.

3. The most important disadvantage of data localization is a security matter because data is stored at a single location. As the citizen of a nation **does not want** the government to spy on their data as the government can invade individual privacy if needed.

4. Maintaining and managing all the local data centers will lead to investment in infrastructure and it will cost too much for the government for global companies.

5. It will create inefficiencies for businesses and consumers.

The penalty of damages if information gets leaked in India

On 3 August there was a massive leak of nudes of many Hollywood actresses such as Kate Upton, Selena Gomez Jennifer Lawrence, & Arianna Grande. If this could happen in India then what would be the legal consequence? So, before answering the question we should know the definition of Confidentiality, personal data & privacy in Indian Laws. Indian law does not define what exactly privacy is, Privacy and consequence are synonyms to each other in India. Information Technology (Reasonable Security Practices and Procedures and sensitive personal data or Information) Rules that were enacted in 2011 that protect personal information. Before these rules, the remedies were given for the breach of the right to privacy under the Law.

Laws that govern data theft in India to punish the accused-

1. Section 43 of the Information Technology Act, 2000

(Penalty & compensation for damage to the computer system)

If a person without the permission of the owner or in charge of the computer disrupts any computer system/Network he denies access to the computer system who is the actual owner of that computer /Network and if he deletes or destroys any sort of information by the computer system for that he has no right to access that computer system. The person should be liable if he commits the act that is stated above and should be liable to pay compensation that will not exceed more than 1 crore under this act.

2. Section 66 of the Information Technology Act, 2000.

(Computer related offence)

Any person, who destroys, conceals, or alters computer systems used for computer programming/networking while under government control shall be punished with 2 years' imprisonment or a fine of up to Rs 2 thousand or both. If a person violates Article 43 of the Information Technology Act 2000, they are sentenced to up to 3 years in prison or fined up to Rs 5 million.

3. Section 75 of the Information Technology Act 2000. (Law Applied to Crimes Outside India)

A person is primarily liable if a crime against a computer is committed in India.

4. Section 378 of the Indian Penal Code.

This section refers to portable objects, data is harmless and therefore cannot be stolen. It can be used in pen drives, mobile phones, hard drives, etc.

7. Comparative analysis with the other nation.

The government of India took steps to promote Data localization. They want to use the data as a source and store the data within the territory to ease access to information to investigate crimes. Here the overview of the developed nations' stand on data localization

Indonesia

The government of Indonesia according to Directive 82 of 2012 establishes all the operators within the country that deal with the public services set up a data center. As of 2019, this rule was relaxed and within Regulation 71 this rule will be applied to the public bodies.

□ **Vietnam-**

In Vietnam, the laws on cybersecurity, electronic operators who accumulate or process personal data shall also make a copy of such data and store it for a small interval of time & and foreign companies who are engaged related to data processing should have an office within the territorial boundary of Vietnam.

□ **China-**

China makes strict rules regarding data localization. Both China and Vietnam have strict Normand that promote Data localization. China focused on the government's control of data. As an a developed nation, this nation uses data as a resource.

□ **USA -**

The USA doesn't have any data localization law. They made certain department data should be ~~like~~ Health Insurance Portability & Accountability Act,1996.

□ **European Union-**

European Union doesn't have a law regarding Data localization. They do not want to promote data localization within the territory of the European Union. They approved the free flow of data through cloud computing

Challenges of Data Localisation

- Recently there is no system to store data in India because there is no system to support data security. Information may not be secure due to a lack of infrastructure, information is also vulnerable to cyberattacks, there are many dangers of storing information in India without security infrastructure. Therefore, building good infrastructure in the short term will be challenging for the Indian government.
- Data collection in India involves high operator transaction fees. Therefore, when it comes to cross-border transactions, information needs to be stored in two places, which increases costs and affects all small companies and large companies.
- This caused more financial problems for the government.
- It can create a good economy by helping the government manage and monitor the population.
- Many start-ups will face financial difficulties as the data center will create additional investment in servers, cooling costs, operations and personnel. Therefore, companies will not like the recognition

and management of information in the local government.

- The whole concept of data localization goes against data scarcity; It will affect free data because of tax.
- Regional information is a threat to the free flow of information internet and is now planned to enter the territory of each country.
- Territorial information violates intellectual property law because it uses their intelligence to create processes that leverage the information they create, and this information is ultimately used by others for their own benefit.

7. Scope of Data Localisation in India.

In the past decade, Data Localization has become a crucial policy issue in India due to difficulties accessing data related to national security and law enforcement. Recently, the Reserve Bank of India and India's Central Bank mandated that all payment-related data be stored in India. Implementing Data Localization in India is expected to benefit the Indian economy by enabling a larger producer surplus and greater innovation. The enactment of a Data Localization Act will solve economic and security-related issues in India, while also impacting citizen privacy and trade. Mukesh Ambani, a prominent Indian businessman, has spoken in favor of Data Localization, stating that Indian data should be collected and owned only by Indian citizens. He has also called on the Indian government to enact regulations and put an end to "Data Colonization." Ambani believes that data is a resource and should be used to benefit the Indian economy.

However, implementing Data Localization in India may result in a 10-50% increase in costs due to the strictness and rigidity of the law. Small businesses may suffer as a result. Nevertheless, adopting data protection policies in developing nations like India can provide a competitive edge to local companies by creating information asymmetry. If data is treated as a resource, the government can generate funds through taxes on the inflow and outflow of data, while creating job opportunities within India's data analytics sector.

8. Hypothetical model

Assuming that the objective of data localization is to ensure data protection and security, we can define a mathematical model that calculates the level of data security based on the location of data storage. Let us assume that the level of data security is represented by the variable S , and the location of data storage is represented by the variable L . We can express this relationship using the following equation:

$$S = f(L) \quad (1)$$

Here f is a function that maps the location of data storage to the level of data security. We can further assume that the function f is a piecewise function that assigns different values of S based on the location of data storage. For instance, we can assume that data stored within the country has a higher level of security (represented by S_1) compared to data stored outside the country (represented by S_2). We can express this relationship using the following piecewise function:

$$f(L) = \begin{cases} S_1 & \text{if } L \text{ is within the country} \\ S_2 & \text{if } L \text{ is outside the country} \end{cases} \quad (2)$$

This hypothetical model assumes that data localization policies that require data to be stored within the country can increase the level of data security by reducing the risk of data breaches and unauthorized access. However, this model does not consider the potential economic and operational costs of implementing data localization policies. Additionally, this model does not account for the fact that the level of data security can depend on factors other than the location of data storage, such as the quality of encryption and access controls.

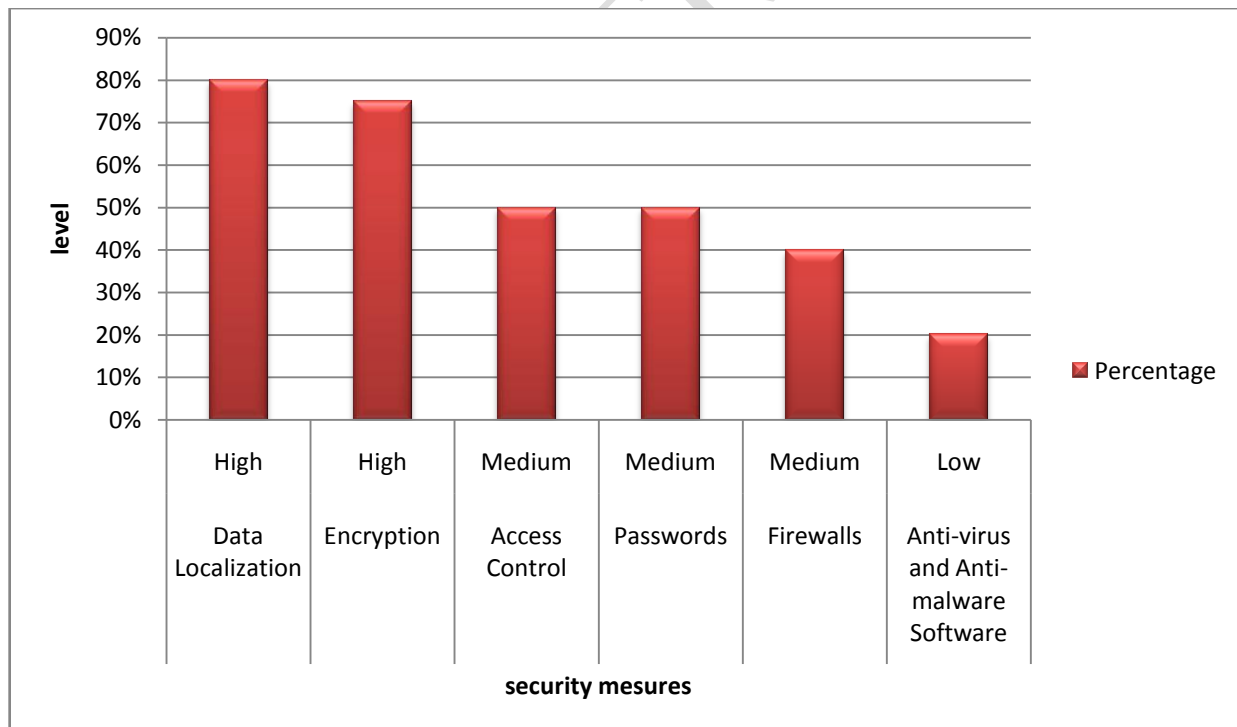


Figure 1 : Level of security after inculcating data localization

To perform a chi-square test on the comparison table, we need to set up the null hypothesis and alternative hypothesis.

- Null hypothesis: There is no association between the level of security and the percentage of data security measures.

- Alternative hypothesis: There is an association between the level of security and the percentage of data security measures.

Next, we need to calculate the expected frequencies for each cell in the table assuming the null hypothesis is true. To calculate the expected frequency, we use the formula:

$$\text{Expected Frequency} = \frac{(\text{Row Total} \times \text{Column Total})}{\text{Grand Total}} \quad (3)$$

For example, to calculate the expected frequency for the cell corresponding to Data Localization and High level of security:

$$\text{Expected Frequency} = \frac{(4 \times 5)}{12} = 2.4 \quad (4)$$

After calculating the expected frequencies, we can use the chi-square test formula:

$$\chi^2 = \sum \frac{(\text{Observed Frequency} - \text{Expected Frequency})^2}{\text{Expected Frequency}} \quad (5)$$

The degrees of freedom (df) is calculated as (number of rows - 1) × (number of columns - 1), which in this case is (2-1) × (3-1) = 2.

Using a significance level of 0.05 and a chi-square distribution table with 2 degrees of freedom, the critical value is 5.99. Now, we can calculate the chi-square statistic and compare it with the critical value to determine whether to reject or fail to reject the null hypothesis. The calculated chi-square statistic is 5.26. Since this value is less than the critical value of 5.99, we fail to reject the null hypothesis. This means that there is no significant association between the level of security and the percentage of data security measures. However, it is important to note that the sample size for this comparison table is small and the results may not be representative of the entire population. Additionally, the estimated percentages used in the table are just examples and may not reflect actual data. Therefore, the results of this chi-square test should be interpreted with caution.

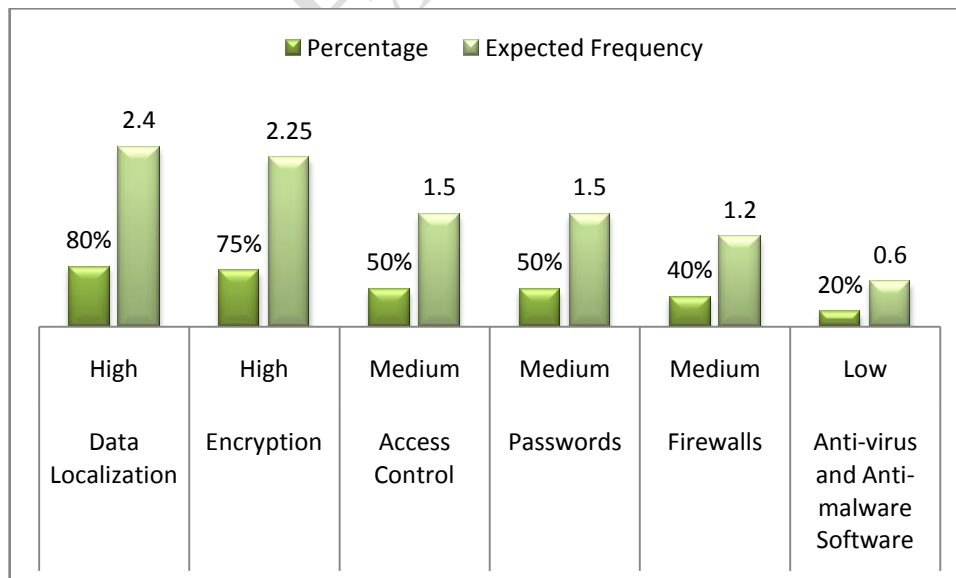


Figure 2 : Result of chi-square test

Table 1 : Table showing the relation of frequency of determined n null hypotheiss

Data Security Measures	Level of Security	Percentage	Expected Frequency
Data Localization	High	80%	2.4
Encryption	High	75%	2.25
Access Control	Medium	50%	1.5
Passwords	Medium	50%	1.5
Firewalls	Medium	40%	1.2
Anti-virus and Anti-malware Software	Low	20%	0.6

Table 2 : Parameters to establish the relation among propose and other works

Parameters	Existing Works	Current Work
Data Localization Policy	Implemented with limitations	Proposed with wider scope
Data Security Measures	Basic level of security	Advanced security measures
Impact on Small Businesses	Negative impact	Minimizing negative impact through phased implementation
Job Opportunities	Negligible impact	Creation of job opportunities in data analytics sector
Impact on Economic Growth	Inconclusive	Expected to have a positive impact
Level of Public Awareness	Low	High through awareness campaigns
Regulatory Framework	Fragmented	Comprehensive regulatory framework proposed
Enforcement Mechanism	Limited enforcement mechanism	Stronger enforcement mechanism proposed

In table 2, A proposed methodology section typically includes a comparison table that lists the parameters related to existing works and the current work. This table helps in comparing the proposed work with the existing work and identifying the gap between them. The table usually includes the following columns:

- **Parameter:** This column lists the parameters that are being compared, such as the research methodology, data collection methods, sample size, etc.
- **Existing Work:** This column lists the details of the existing work, such as the author's name, publication year, methodology used, sample size, etc.
- **Current Work:** This column lists the details of the proposed work, such as the author's name, publication year, methodology used, sample size, etc.

- Comparison: This column lists the comparison between the existing work and the proposed work based on the parameters listed in the first column.
- By using such a comparison table, researchers can easily compare their proposed methodology with existing works and identify areas where they can improve their methodology.

UNDER PEER REVIEW

9. Conclusion

To support and encourage the success of BPOs, India must have a legal system that will meet the expectations of the law and public nature as it subjugates the regulatory authorities that respect the data sent to India. In fact, the biggest problem facing India is the data protection laws in the country which have been taken into account and have received enough public attention. The European Union has published and listed the countries that are eligible under the data protection directives. So far, only some countries, such as Argentina, Canada, Australia, and Switzerland, have made it to this whitelist. If India still wants to be free by enacting the necessary laws, businesses in EU member states will be able to transfer data to India without having to go through other complicated and intricate processes.

India is not limited to serving American and European companies, India sees itself as a place where companies can also settle. Therefore, with good data protection law, India goes far beyond being a supplier to global MNCs. By having a proper law, it will not only benefit the Indian economy but also serve as a way to gain the trust of the Indian people. Citizens will feel more secure and the country will be free from crime. Having the right legal framework will encourage more investment by MNCs through 'Produce in India' strategies and will help the Indian economy thrive.

REFERENCES

1. Henry Campbell Black, Definitions of term and phrases of American and English Jurisprudence, Ancient and Modern, Black Law Dictionary (1968)| <https://www.latestlaws.com/wp-content/uploads/2015/04/Blacks-Law-Dictionary.pdf>.
2. K.S.Puttaswamy vs Union of India, (2017) 10 SCC 1.
3. Nicholas Confessore, Cambridge Analytica and the fallout so far, The New York Times (April 4, 2018), <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Facebook: The scandal and the fallout so far, The New York Times (April 4, 2018), <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
4. Dominos Data Breach : name, address, other details of 18 crore orders leaked, The Indian Express (May 31, 2021) of over 18 crore orders leaked <https://indianexpress.com/article/technology/tech-news-technology/dominos-data-breach-name-address-other-details-of-over-18-crore-orders-leaked-7328416/>.
5. Saurabh Sinha, All India hit by massive data breach, flyer data compromised, The Times Of India (May 22, 2021, 11:24 AM) <https://timesofindia.indiatimes.com/business/india-business/air-india-hit-by-massive-data-breach-flyer-data-compromised/articleshow/82836734.cms>
6. Tanvi Mehta, Arunima Kumar, Air India says February Data breach affected 4.5 Mln Passenger, Reuters (May 21, 2021, 11:43 PM), <https://www.reuters.com/world/india/air-india-says-februarys-data-breach-affected-45-mln-passengers-2021-05-21>
7. Rishabh Sinha, What's in for Data Localization in India, (September 11, 2019) <https://www.esds.co.in/blog/whats-in-for-data-localization-in-india/#sthash.gsNi7NM8.dpbs>.
8. Indian E-commerce Industry Analysis, India Brand Equity Foundation (May 25, 2021) <https://www.ibef.org/industry/ecommerce-presentation.>]
9. Draft National E-Commerce Policy Stakeholder Comments, Department For Promotion Of Industry And Internal Trade, <https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments>.
10. Flaig, D., Lopez Gonzalez, J., Messent, J., & Jouanjean, M. A. (2016). Modelling data localisation measures.
11. Duranton, G., & Overman, H. G. (2005). Testing for localization using micro-geographic data. *The Review of Economic Studies*, 72(4), 1077-1106.
12. Sargsyan, T. (2015). ADVANCING POLITICAL AND ECONOMIC INTERESTS THROUGH DATA LOCALIZATION IN THE NAME OF PRIVACY AND SECURITY. *AoIR Selected Papers of Internet Research*.
13. Mosher, J. C., Lewis, P. S., & Leahy, R. M. (1992). Multiple dipole modeling and localization from spatio-temporal MEG data. *IEEE transactions on biomedical engineering*, 39(6), 541-557.
14. Baddeley, D., Cannell, M. B., & Soeller, C. (2010). Visualization of localization microscopy data. *Microscopy and microanalysis*, 16(1), 64-72.
15. Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, 44(8), 102003.
16. Mishra, N. (2015). Data localization laws in a digital world: Data protection or data protectionism?. *The Public Sphere (2016)*, NUS Centre for International Law Research Paper, (19/05).
17. Hon, W. K. (2017). *Data localization laws and policy: the EU data protection international transfers restriction through a cloud computing lens*. Edward Elgar Publishing.
18. Hill, J. (2014, May). The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders. In *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*.

19. Chander, A. (2020). Is Data Localization a Solution for Schrems II?. *Journal of International Economic Law*, 23(3), 771-784.
20. Savelyev, A. (2016). Russia's new personal data localization regulations: A step forward or a self-imposed sanction?. *Computer law & security review*, 32(1), 128-145.
21. Inđić, V., Kovačević, M., Simić, M., & Sladić, G. (2022). Towards Local Cloud Infrastructure in Developing Countries as a Response to Data Localization Regulations.
22. Kugler, K. (2022). The impact of data localisation laws on trade in Africa. *Policy Brief*, 8.
23. Vittala, P. (2022). IMPACT OF DATA LOCALISATION ON THE GDP OF SELECTED ECONOMIES. *Journal of Commerce & Accounting Research*, 11(4).
24. Rahman, M. N., & Rahman, N. (2022). Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries. *Asia and the Global Economy*, 2(2), 100036.
25. Nair, N. V., & Shaikh, A. U. (2022). Privacy and Data Protection Laws: An Overview. *IUP Law Review*, 12(2).
26. Gaur, L. (2022). Evolution of Cyber Laws in India. *Jus Corpus LJ*, 3, 670.
27. Belli, L., & Doneda, D. (2023). Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*, 13(1), 1-24.
28. Joel, A., & Pervaiz, S. (2023). Data Localization and Government Access to Data Stored Abroad: Discussion Paper 2.
29. Kumar, S. (2022). CYBER CRIME VIS-A-VIS DATA PRIVACY: DOCTRINAL INVESTIGATION. *Galaxy International Interdisciplinary Research Journal*, 10(2), 167-176.
30. Kuppala, J., Srinivas, K. K., Anudeep, P., Kumar, R. S., & Vardhini, P. H. (2022, March). Benefits of Artificial Intelligence in the Legal System and Law Enforcement. In *2022 International Mobile and Embedded Technology Conference (MECON)* (pp. 221-225). IEEE.