NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

Does Data Localization Measures Really Enhance Law Enforcement?

G. Mahith VidyaSagar, Advocate High Court of Andhra Pradesh.

ABSTRACT

The concept of data localization is a debatable subject globally India is no exception. Basically, data localization means adopting the measures to store the data pertaining to a country within the country itself. Data localization acts as a barrier to cross border data flow which was the primary concern of many developed countries like the U.S and Japan. In recent times the debates around data localization raged across the world because not only the authoritarian governments like China but also the democratic countries like India also intend to adopt data localization for various reasons. However, the steps towards data localization by India, even supported by certain legitimate contentions, further raises certain legal questions pertaining to the data protection of the individuals. Those steps also question the technical feasibility of India. Recently the two initiatives of India towards data localization i.e. the provisions relating to data localization in the Data Protection Bill and, the RBI directive ordering for storing and processing of data relating to the payments sector gained global attention. The directive just mandated the storage and processing of data but it does not contain any guidelines in relation to that. The readiness for compliance of a policy is needed to check before going to adopt it. As far as the RBI directive is concerned it has been opined that it does not check the possibility of keeping up pace with that localization requirement.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

Table of Contents

I. INTRODUCTION 3

II. CONCEPT OF DATA LOCALISATION 4

III. LAW ENFORCEMENT AND DATA LOCALISATION 7

IV. CONCLUSION 15

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

I. INTRODUCTION

The concept of data localization is a debatable subject globally India is no exception. The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are constructing borders in cyberspace, breaking apart the World Wide Web.[1] Because of these issues now, the international community is driving towards the concept of storing data belonging to a nation within its borders only.

Recently the two initiatives of India towards data localization i.e. the provisions relating to data localization in the Data Protection Bill and, the RBI directive ordering for storing and processing of data relating to the payments sector gained global attention. The directive says:

All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system ***only in India****. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required*.[2]

The directive just mandated the storage and processing of data but it does not contain any guidelines in relation to that. The readiness for compliance of a policy is needed to check before going to adopt it. As far as the RBI directive is concerned it has been opined that it does not check the possibility of keeping up pace with that localization requirement.

[1] Anupam Chander & Uyen P. Le, "*Data Nationalism,*" 64 EMORY L.J. 677 (2015).

[2] STORAGE OF PAYMENT SYSTEM DATA, RBI/2017-18/153, DPSS.CO.OD No.2785/06.08.005/2017-2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

The data localization measures will eventually create a situation, where data examination will be done at the national borders, in order to check whether it is allowed to leave the country and possibly taxed when it does. Creation of national barriers to data by adopting data localization measures might break up the World Wide Web, which was designed to share information across the globe.[3] Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders.[4]

Against this background an attempt has been put forward by this article to study the arguments supportive to data localization, *i.e., data localization enhances the law enforcement*. For that purpose, this article is divided into two three parts. Part I deals with the introductory part. Part II explains the meaning and definition of data localization. Part III analyses the issue of law enforcement and data localization.

II. CONCEPT OF DATA LOCALIZATION

In order to address the wide range of ' logistical, privacy and security challenges,' put forth by the increase in growth and diversification of digital data, governments across the world have struggled over the course of recent decades, especially since the commercialization of the internet in the early 1990s.[5] At present, law of the States which is coupled with the concerns of security, data theft, surveillance by foreign states, and enforcement of law, breaking the World Wide Web apart and constructing borders, check points for the data to pass out of the state. Internet border controls

[3] *See* Tim Berners-Lee with Mark Fischetti, 4 *Weaving The Web: The Original Design and Ultimate Destiny of The World Wide Web by its Inventor* (1999) (describing a vision of a "single, global information space").
[4] *See* Ethan Zuckerman & Andrew Mclaughlin, *Introduction to Internet Architecture and Institutions"* (2003), http://cyber.law.harvard.edu/digitaldemocmcy/internetarchitecture pdf.
[5] Jonah Hill Force, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,* at 3 (The Hague Institute for Global Justice, May 1, 2014). Available at SSRN: https://ssrn.com/abstract=2430275

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

of first generation tried to keep information out of a country-from Nazi paraphernalia to copyright infringing material.[6] But the latest generation of Internet Protocols wants, not to store the data out but rather to keep it in. This storing of data within a nation or a state or a territory is termed to be as data localization.

Data localization can be described as:

"....measures that limit the data storage, moment and/or processing of data to specific geographies and jurisdictions or that limit the companies that can manage data based upon the company's nation of incorporation or principal sites of operation and management."[7]

It means data localization means the measures adopted for limiting the storage, moment or processing of data pertaining to specific jurisdiction or limiting the companies that can manage the data based on the company's nationality or principal seat of operation and management.

Data Localization measures has been defined as

> *.... [T]hose that specifically encumber the transfer of data across national borders These measures take a wide variety of forms-including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data*. [8]

[6] *See* Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, D. 2000 inf. rap. 172, obs. J. Gomez, *available at* http://juiscom.net/2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licm-c-yahoo-inc-et-yahoo-france/, *translation available at* http://www.lapres.net/yahen.html (Daniel Arthur Lapr&s, trans.); Tribunal de gmnde instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, JCP 2000, Actu., 2219, obs. J. Gomez (Fr.), *available at* http://juiscom.net/wp-content/documents/tgiparis20001120.pdf, *translation available at* http://www.lapres.net/yahenll.html (Daniel Arthur Lapr&s,trans.); *see also* Yahoo! Inc. v. La Ligue Cotnre le Racisme et L'Antisemtisime, 433 F.3d 1199 (9th Cir. 2006) (en banc) (per curiam) (discussing the French proceedings and parallel proceedings in the United States). For a domestic example, see Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011), which was ostensibly designed to require internet service providers to block access to foreign websites hosting copyright infringing materials.

[7] Helena Urisc et. al., *Data Localisation measures and their Impacts on Data Science, in* HANDBOOK on DATA SCIENCE AND LAW (Edward Elgar eds, 2018), available at SSRN: https://ssrn.com/abstract=3102890.

[8] *See* Chander & Uyen, *supra* note 1, at 680.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

It was argued that *storing of data within the national jurisdictions or restricting it from passing through a territory or infrastructure of untrustworthy nations or those nations' technology companies*- data will be protected better and the foreign surveillance will be better curtailed.[9] This eventually made the governments across the world make efforts to keep data within the national borders to avoid the foreign surveillance but at the same time it is giving wider powers to the government which might hamper the privacy of the individuals. At the same time, another aspect is added to this debate that is- the construction of borders for the flow of data will act as a barrier for trade which is dependent on cross-border data flow.

Today, both the developed and developing countries have introduced or are actively considering introducing data localization laws and policies relating. These laws, regulations and policies which are under considerations are varied in their application and effects. Some proposals would put some restrictions on data storage, transfer and processing, while others require the local purchasing of ICT equipment for the Government and private sectors procurements. There are certain proposals which mandate compulsory ownership of equipment to store data, restrictions on online traders and forced local hiring.[10]

Proposals of this kind are not new. In fact, over years the forms of data localization policies have been in place actively in different countries.[11] Authoritarian Governments like China, Russia and Iran, have intended to pursue broader localizing rules to make them applicable to all its citizens- the effective measure to monitor the activities of citizens data localization rules are best. However, even the democratic countries- most notably, Brazil, India and Germany- are now seriously considering these expansive data localization laws, post-Snowden revelations.[12]

[9] Jonah Hill Force, *supra* note 5, at 3.
[10] *Id.*
[11] *See* Chander & Uyen, *supra* note 1, at 682-708, where data localisation measures that are adopted in 14 jurisdictions such as- *Australia, Brazil, Canada, China, European Union, France, Germany, India, Indonesia, Malaysia, Nigeria, Russia, South Korea and Vietnam*- have been discussed.
[12] Jonah Hill Force, *supra* note 5, at 4.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

The most recent example of India's willingness to implement data localization policies is its refusal to become a signatory to ***Osaka Track***[13]- which is launched in the ***G20 Summit*** held in June, 2019. The declaration was pushed by Japan along with the United States for the promotion of cross-border data flow with enhanced protection. The major contention put forth by the Indian Government for implementing data localization measures was they increase the law enforcement. This raises a question of the legislative preparedness to deal with the legal complexities associated with data localization. This argument has been analyzed in the following section.

III. LAW ENFORCEMENT AND DATA LOCALIZATION

Regulation of cross-border data flow is being noticed as a major global tussle in 2019, with most emerging economies adopting measures to exercise greater control over their data. The study conducted by *The Centre for Internet and Society*,[14] identified that- China, India, Indonesia and Vietnam are the important Asian countries that already had existing or proposed laws mandating data localization in some form. If only India is considered its data localization gambit started with the issuance of the directive of Reserve Bank of India (RBI) on Apr. 6, 2018 imposing strict data localization requirements to be complied with, by Payment System Operators.[15] Since then there has been notifications from eight sectors mandating data localization in some form- from regulators governing insurance, healthcare, and e-commerce sectors.[16]

[13] Osaka Declaration on Digital Economy, Jun. 28, 2019. Available at https://www.wto.org/english/news_e/news19_e/osaka_declration_on_digital_economy_e.pdf

[14] Arindrajit Basu et. al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India* (Pranav M Bidrae et. al. eds., The Centre for Internet Society, Mar. 19, 2019).

[15] STORAGE OF PAYMENT SYSTEM DATA, RBI/2017-18/153, DPSS.CO.OD No.2785/06.08.005/2017-2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[16] Arindrajit Basu, The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam, The Diplomat, Jan. 10, 2020 available at https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

However, the global attention attained with the introduction of *mirroring provision* in the draft of ***Personal Data Protection Bill,*** made public in August 2018, which mandated a live serving copy of all the personal data be stored in India, and all the data notified as *"critical personal data"* was restricted from the cross-border data transfer.[17] But, in the final revised version of the Bill that was introduced in Parliament in December, 2019, the mirroring provision was removed.[18]

The arguments advanced in favour of implementing stringent data localization norms are broadly divided into three sets: Sovereignty and government functions; referring to the need to recognize Indian data as a resource to be used to further national interest (economically and strategically), and to enable enforcement of Indian law and State functions. Accruing of economic benefits to the local industry in terms of local infrastructure creation, employment and contribution to the AI ecosystem- is the second claim. Finally, pertaining to the protection of civil liberties, it has been argued that local hosting of data will enhance the privacy and security by ensuring the application of Indian Law to the data there is an opportunity for the users to access local remedies.

Enacting data localization measures may help in ensuring the protection of the rights of data subjects in some circumstances. For instance, in the Microsoft case, it was held that the US's Stored Communications Act cannot be applied extraterritorially, and can only be applied to data which is actually stored in the country.[19] This case referred to whether the government, by way of a warrant issued under the Stored Communications Act could request Microsoft to access and produce emails of a customer whose data was stored on a server in Ireland.[20]

Data localization makes the data available for the requirement of domestic law enforcement. Since enforcement jurisdiction is primarily territorial, the location of assets or equipment in the jurisdiction can be justified as a way to make it easier to enforce local law.[21] There are many instances where Government agencies had expressed their dismay in securing the compliances

[17] THE PERSONAL DATA PROTECTION BILL, 2018, § 40. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[18] THE PERSONAL DATA PROTECTION BILL, 2019, Bill No. 373/2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. In this bill Chapter VII deals with the Restriction on Transfer of Personal Data outside India.
[19] Microsoft Corporation v. United States of America, No. 14-2985 (2d Cir. 2016).
[20] *Id.*
[21] Christopher Kuner, *Data Nationalism and its Discontents*, 64 EMROY L. J. 2089, 2094 (2015).

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

with the requirements of domestic law by the Internet-based services.[22] The problems faced for conducting cyber-crimes investigation had been referred by the *Madras High Court* in the ***Blue Whale Case.***[23] In the words of the Court:

> *Cyber investigation is still at a nascent stage in India. The investigators are often at a dead - end because they have neither the access to the communication inside the OTT services/social networking sites nor could they collect the crucial user information required for investigation from the anonymous service providers. For instance, no one knows who is operating "Telegram". It does not have a nodal officer who can be called upon to comply with the directives that may be issued by the law enforcement agencies. Even if they are available in India, they tend to take the stand that the OTT service/social networking service is provided by another company incorporated in USA or any other foreign country and that therefore they are not in a position to furnish the information sought for. They also claim that they do not have the obligation to comply with the directions issued by the Indian Authorities.*[24]

In this case the Court also re-read the response given by *Google India* for the letter addressed to it by the MeitY seeking to un-list/remove the said game/apps from relevant platforms like Google Play store for avoiding the further downloads.[25] But *Google India* had virtually washed its hands off stating that the action will be provided by the Google Play Team in the USA if their policy is violated.[26]

The above referred case is no way connected with data localization but in this case the Hon'ble Court highlighted the problems in investigating the cyber-crimes and the difficulties in collection of data stored in foreign jurisdictions to carry out the law enforcement. It shows the seriousness of the problems in investigating and to enforce the State functions regarding cyber offences. This argument drives support for data localization.

---

[22] Rishab Bailey & Smriti Parsheera, *Data localisation in India: Questioning the means and ends, (*NIPFP Working paper series 242), at 27.
[23] The Registrar (Judicial) v. The Secretary to Government, 8 MLJ 712 (2017).
[24] *Id.,* ¶ 16.
[25] *Id.,* ¶ 9.
[26] *Id.,* ¶ 10.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

If a certain action committed online is an offence in India and the authorities want to take legal action against it, and asking the intermediaries to take necessary action against, the intermediaries are contending that it is not an offence under the other laws and the compliance of India's order globally will result in conflict of laws. The same contention was raised by *Facebook* in the defamation case filed against it by *Yoga Guru Rmadev*. [27] In this case the *Yoga Guru Ramdev* filed a suit seeking for the global removal of a defamatory video published against him and the re-uploaded versions of the same from various social media platforms. Being one of the defendants, *Facebook* had submitted that what constitutes defamatory will differs from country to county and also stated that in … *[U.K.], the onus is upon the Defendants to show that the content is not defamatory. However, in the U.S., the onus on the Plaintiff in a defamation action is very high. Defamation laws differ from jurisdiction to jurisdiction, and therefore, passing of a global disabling order would be contrary to the principle of comity of Courts and would result in conflict of laws.*[28]

The court disagreed with the contentions of the defendants and ordered for a global removal of the defamatory published against the *Yoga Guru* not only from *Facebook* but also from *Google* as well as *Twitter*. This was the decision given by *Prathiba M. Singh, J*- single judge bench of Delhi High Court. Even though the plaintiff in the present case was succeeded but the order of the Delhi High Court raised the debate of the application of *long-arms rule* and the question of implication of such order in the countries where there is liberal free speech jurisprudence.

One of reasons for granting global removal order rather than geo-blocking measures was, if it was removed from accessing India the people from India can still have the access to it by using VPNs.

There are a lot of instances where the Government agencies faced problems while discharging their duties. One such instance is the issue that had happened with the ***Blackberry*** after 2008 Mumbai Attacks. In Mumbai 2008, attacks the terrorists used ***Blackberry*** devices for communication and the encryption system of ***Blackberry*** is highly secured and it becomes hard for the security agencies to decrypt it and sought the help of the company. But the company declined the request of the security agency stating that it is against their consumer privacy policy. As a result the Indian Government required access to data of telecommunication providers and

[27] Swami Ramdev and Ors. v. Facebook, Inc and Ors., 2019 (178) DRLJ 151.
[28] *Id.*, ¶ 10.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

certain telecommunication providers were asked to locate servers in India for facilitating data access for law enforcement.[29]

Likewise, on many occasions India asked the Government of the U.S. to summon *Google, Facebook, Twitter* and others for failure on their part for dissemination of speech prohibited under the Indian law, but considering the U.S. civil liberties those requests were declined.[30]

Currently, jurisdictional claims against foreign entities are enforced through *Mutual Legal Assistance Treaties (MLAT)*.[31] The presence of personal information in the territory of a country could trigger the territorial basis for jurisdiction, thus giving additional powers to police and other law enforcement agencies. If data is locally stored in India, enforcement agencies will have access to a larger pool of data. This data could aid counter-terrorism efforts and may help protect national security. Further, local storage of data will ensure easier access to data in contradistinction to foreign storage of data wherein the sovereign power may choose not to grant access to Indian law enforcement agencies.

It has also to be noted that the agencies of government are also unable to have access to data because of the complexities involved in the *MLAT* procedures and the compliances of legal requirements of the other country for accessing data required.[32] No doubt law enforcement is a laudable goal of data localization, so long as the laws do not violate human rights.[33]

The anonymity feature of the internet is creating complications day by day. To solve all those issues, access to data is necessary for the law enforcing agencies and it could be achieved by data localization measures. However, a mere policy like *RBI Directive*[34] and other sectoral measures *per se* would not be sufficient. Well established legal framework is necessary to deal with the issues associated with it.

[29] Chander & Uyen, *supra* note 1, at 731.
[30] Helena Urisc et. al., *supra* note 7, at 12.
[31] Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 748 (2016).
[32] Bailey & Parsheera, *supra* note 22, at 27.

[33] Chander & Uyen *supra* note 1, at 733.
[34] STORAGE OF PAYMENT SYSTEM DATA, RBI/2017-18/153, DPSS.CO.OD No.2785/06.08.005/2017-2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

The data localization might help in effective law enforcement but at the same time it may also grant arbitrary power to the Government over the data. Why because when we look at sec. 69 of the IT Act, 2000 it empowers the Central Government or State Government or any officer specifically authorised on its behalf can direct any agency of the appropriate government to intercept, monitor, or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer source in the interest of the sovereignty or integrity of the country, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to the above mentioned or for investigation of any offence. This provision might turn into a monster if data localization measures have been adopted without a legal framework that limits the powers of Government and its agencies over the data. Showing the reasons that are mentioned in the above referred section the Government and its agencies might process each and every bit of the data stored in the country and will peek into each individual life. It might hamper the information privacy of the citizens'. Which tends to be recognised as facet of the right to privacy by the Hon'ble Supreme Court in the landmark judgment of *Puttaswamy.*[35] The data localization measures bring the data under the control of the local authorities in such a situation it will be justifiable if the Government and its agencies exercise the powers conferred under sec. 63 for legitimate purposes but if it goes beyond individual fundamental rights will be at stake. In other words there needs a restriction for the usage of data by the Government. It means enhanced data protection principles have to be designed to protect the personal information of the individuals by restricting how such information can be collected, used and disclosed by the Government and its agencies.

When we are talking about the data protection there is no comprehensive mechanism in India, excluding the *Data Protection Bill, 2019* because it is yet to be enacted into an Act. Currently, the primary enactment that deals with data protection is IT Act, 2000 and the rules made there under. The *Information Technology (Reasonably Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 [IT Rules],* deals with the protection of individual data. Under

[35] Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

IT Rules *personal information*[36] and *sensitive personal data or information*[37] is sought to be protected. The SPDI Rules have been issued under Section 43A of the IT Act. Section 43A, relates to ―Compensation for Failure to Protect Data‖ and enables the enactment of reasonable security practices and procedures‖ for the protection of sensitive personal data. The SPDI Rules incorporate, to a limited extent, the OECD Guidelines, specifically: collection limitation, purpose specification, use limitation and individual participation.

The SPDI Rules mandate certain requirements for the collection of information,[38] and insist that it be done only for a lawful purpose connected with the function of the organisation.[39] In addition, every organisation is required to have a detailed privacy policy.[40] The SPDI Rules also set out instructions for the period of time information can be retained,[41] and gives individuals the right to correct their information.[42] Disclosure is not permitted without consent of the provider of the individual, or unless such disclosure is contractually permitted or necessary for legal compliance.[43] When it comes to sharing information with Government agencies, then the consent of the provider is not required and such information can be shared for purposes such as verification of identity, prevention, detection and investigation including cyber incidents, prosecution, and punishment of offences.[44]

The SPDI Rules apply only to corporate entities[45] and leaves the government and government bodies outside its ambit; the rules are restricted to sensitive personal data, which includes attributes like sexual orientation, medical records and history, biometric information etc.,[46] and not to the larger category of personal data.

[36] INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011- rule 2(i) [IT Rules].
[37] IT Rules- rule 3.
[38] Rule 5(1), SPDI Rules.
[39] Rule 5(2), SPDI Rules.
[40] Rule 4, SPDI Rules.
[41] Rule 5(4), SPDI Rules.
[42] Rule 5(6), SPDI Rules.
[43] Rule 6, SPDI Rules.
[44] Rule 6(1), SPDI Rules.
[45] Section 43-A, IT Act.
[46] SPDI Rules, Rule 3

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

If data localization measures are adopted in different sectors the processing of data for a plethora of purposes by Government and its agencies will increase, however the present legal framework pertaining to data protection does not apply to them.

This argument shows that the supporting statement of data localization- i.e. data localization helps in the enforcement of domestic law- further raises certain legal questions for which the current legislative mechanism in India could not have answers.

In other words the legal framework in India is currently not well equipped to answer the legal problems that are integrated with data localization. To answer all those problems and to proceed with the data localization norms India needs a comprehensive and detailed law relating to data protection.

Even though *Data Protection Bill, 2019* came up as comprehensive legislation to deal with the issues in relation to data protection and in the bill laid down the certain obligations[47] on *data fiduciaries*[48]-includes Government and its agencies that deals with data-for data protection. It is still yet to be enacted into an Act. Currently it is under the scrutiny of the Parliamentary Committee. Hence, the preparedness of the *Data Protection Bill* to answer all the questions put forth by data localization and its effective implementation could also be doubted.

[47] *See* THE PERSONAL DATA PROTECTION BILL, 2019, Bill No. 373/2019, § 4 to 11 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[48] *Id.,* § 2(13)- "data fiduciary" means any person, including State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing personal data.

NLR | NyaayShastra Law Review
ISSN: 2582 -8479
www.nyaayshastra.com

IV. CONCLUSION

It has to be noted that even though the supportive argument for data localization is laudable one the current legal infrastructure has lacunas to resolve certain legal issues that will be posed by the data localization. In India the legal development regarding data protection and its associated issues is still considered to be premature to adopt strict data localization norms. Hence the research hypothesis is proved.

Therefore, based on the above deliberations currently India's adoption of strict data localization measures is not an appreciable policy.

Suggestions

On certain normative grounds, indeed there may be circumstances where data localization measures can be justified. For identifying such situations, and to arrive at a narrowly tailored response, the policy making process should include certain steps. These steps are:

- For making policy mere identification of the problem will not be sufficient. The specific problem which is sought to be addressed must be identified along with the evidence indicating the intensity of the problem.
- Each alternative available to address the issue must be considered along with the expected costs and benefits of each of them.
- Among the range of localization options that are available, the priority should be to begin by considering the least intrusive measure (conditional transfers of data) before moving towards the most onerous requirement of storage and processing only within the territory.
- In order to provide the affected parties and public at large the opportunity to question and strengthen the analysis, the entire process should be put forward in a transparent manner.