III. DATA LOCALIZATION: AN ISSUE BEYOND BORDERS

- Gargi Whorra[*]

ABSTRACT

In modern day, technology driven life, data has acquired a critical position, resulting in an increased assertion for greater control in order to achieve greater digital sovereignty. Therefore, data localization has emerged as a significant policy decision by various nations. However, the data localization approach poses severe limitations and regulatory complexities and at the same time proves ineffective in providing data security, data access and innovation. Therefore, blanket data localization policies might in turn become detrimental depending on the ground realities of each nation. The fact of the matter remains that whether localization of data in general would have any net benefit for the nation is the most pertinent consideration to be assessed.

The primary focus of this paper is to identify a balanced approach for data governance taking into consideration national sovereignty and broader global concerns. This research paper will examine the prevalent forms of data localization while highlighting the various policy considerations underlying the rising data localization surge. Thereafter, it shall evaluate the privacy, security and economic implications and costs to be born in case of such data localization. The paper provides special focus on the prevalent data regulations and data localization policies in India while assessing its potential impact and an insight into the ongoing global interplay with data localization. Lastly, the paper summarises the analysis with policy recommendations premised on the understanding that like-minded nations would work together to arrive at an arrangement that focuses on identifying a workable balance in the coming future.

[*] The author is a Ph.D. scholar at Ram Manohar Lohiya National Law University, Lucknow. Views stated in this paper are personal.

I. INTRODUCTION

Modern-day technology and innovation dictate most aspects of modern life from healthcare to energy, financial transactions to election processes to state a few. These technologies and innovations are heavily data reliant and therefore data has emerged as a global currency. As a result, there is an increased assertion by various countries to harness and exercise greater control over the data of their citizens. This task is particularly important to create greater digital independence, digital sovereignty, and infuse public trust. Thus, data localization has emerged as a significant policy decision by various nations, in response to pressing concerns and to exercise control over data being stored beyond their national jurisdiction.

The attempt to define the term 'data localization' poses a difficulty since its meaning would defer depending on the context in which it is used. However, for general understanding, it may be understood as a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.[1] Data localization generally connotes some form of requirement for the physical storage of data within the borders of a country, limiting the cross-border flow of such data. Therefore, such localization has also been termed as an encumbrance preventing the flow of data beyond national

[1] D Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (2020) OECD Digital Economy Papers, No. 301 <https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en> accessed 24 March 2022.

borders.[2] It poses itself more in terms of an obligation thereby effectively restricting data within a particular place.

The nature of such restriction is identified under two broad categories i.e., strict or conditional.[3] In terms of strict data localization, the mandate can range from local storage and data processing requirements to even complete restrictions on any form of cross-border data flow. Whereas, the conditional data localization mandate provides for cross-border transfer of data only upon fulfilment of certain conditions. Therefore, the focus is to create a legal limitation on the movement of data by imposing requirements that restrict it to remain locally.[4]

A. The Prevalent Forms of Data Localization

Since globally, data localization has acquired different shapes and forms, it is difficult to categorize it in a straight-jacketed manner. As of now, the most stringent form of data localization can be identified where the obligation of hard localization is imposed. This requirement focuses on local storage, local processing, and the local transmission of data. Therefore, the data is restricted within the boundaries of such a nation, and cross-border data

---

[2] A. Chander, U. P. Le, 'Data Nationalism' (2015) 64 Emory LJ 679 <https://ssrn.com/abstract=2577947> accessed 3 May 2022.

[3] M F Ferracane, 'Restrictions on Cross-Border Data Flows: A Taxonomy' (2017) European Centre for International Political Economy Working Paper 1/2017 <https://deliverypdf.ssrn.com/delivery.php?ID=142095081069090008107127093075126113014042095000089091121086085094072015121024010092119034022008009024050127005078105008116025006007037073081010101123094116031123104037082049074084105081126019114000027079089067> accessed 3 May 2022.

[4] J Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (2013) 22 Issues in Technology Innovation <https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf> accessed 3 May 2022.

transfer is either prohibited or strictly regulated.[5] The prime example of such data localization is China which requires personal data from critical information infrastructure (**"CII"**) to be stored within China by a CII operator.[6] Similarly, Russia requires that the personal data of citizens be accumulated, recorded, stored, retrieved, updated, and altered by operators through the database servers located within Russia.[7]

A limited data localization approach that focuses on cross-border data transfer, with conditional requirements to be fulfilled by the transferee entity is also widely prevalent. European Union's General Data Protection Regulation (**"GDPR"**) is the prime example of such localization. Under the GDPR, the European Commission needs to be satisfied that the transferee is located in a territory that meets the adequate level of protection standards. There are certain exceptions to the said rule i.e., where the public interest of the EU or a member state of the EU is involved or to fulfil a contract or where explicit consent is given by the data subject.[8]

B. Determining the Indian Approach

A comparatively less stringent, nevertheless, cumbersome approach is to require companies to maintain a local copy of data within the territory of such nation. India is primarily moving in this direction under the Personal Data

---

[5] Pablo Urbiola and others, 'Data Flows across Borders: Overcoming Data Localization Restrictions' (*Institute of International Finance,* March 2019) <https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf> accessed 27 March 2022.

[6] Cybersecurity Law of People's Republic of China 2017, art 37.

[7] Russian Federal Law No. 242-FZ.

[8] Kurt Wimmer, Gabe Maldoff and Diana Lee, 'Indian Personal Data Protection Bill 2019 vs. GDPR' (*International Association of Privacy Professionals*, March 2020) <https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf> accessed 27 March 2022.

Protection Bill 2019 which requires Sensitive Personal Data to be stored in India.[9] Cross-border transfer of such data would be permissible only when a copy of such data is stored within India and certain mandatory conditions are fulfilled which are:[10]

- Explicit consent from the data principal
- Transfer of such data should be through a contract/intra-group scheme approved by the Data Protection Authority (**"DPA"**) [Or]
    - The transferee country/entity should be included in the list drawn by the Central Government which deems that such a country provides the necessary adequate protection [Or]
    - Where the DPA, in consultation with the Central Government, authorizes such transfer of sensitive personal information for a specific purpose.

There are even stricter restrictions on cross-border transfer of Critical Personal Data barring limited exceptions such as:

- Health emergency
- Request made by a country/entity that the Central Government has deemed the transfer as permissible.[11]

Irrespective of its form, data localization as a tool of "data nationalization" bears its own cost especially when it acts like a non-tariff

[9] The Personal Data Protection Bill 2019 (373 of 2019), cl 33.
[10] ibid, cl 34.
[11] ibid.

barrier to trade.[12] Therefore, concern associated with increasing data localization is not limited to only economic factors but has far-reaching effects on almost every aspect of modern, technology-driven life.

The rising data protectionism as evident in the case of Russia and China and data restrictiveness as in the case of the EU GDPR are both two ends of the spectrum. China has enforced blanket unconditional localization across all sectors including CII, important personal information of a natural person, financial, energy, transport information, etc. Similarly, Russia provides for unconditional localization by mirroring all personal data of their citizens. Whereas EU supports data transfer, provided personal information is transferred only upon the fulfilment of certain prerequisites. However, the focus of the present discourse lies in between the spectrum, towards countries such as India that are still to determine their policy in terms of data governance and localization. In the long run, the development of policies by such countries will prove vital in determining the future of the global digital economy and the nature of the internet as either open and regulated or as closed and controlled.

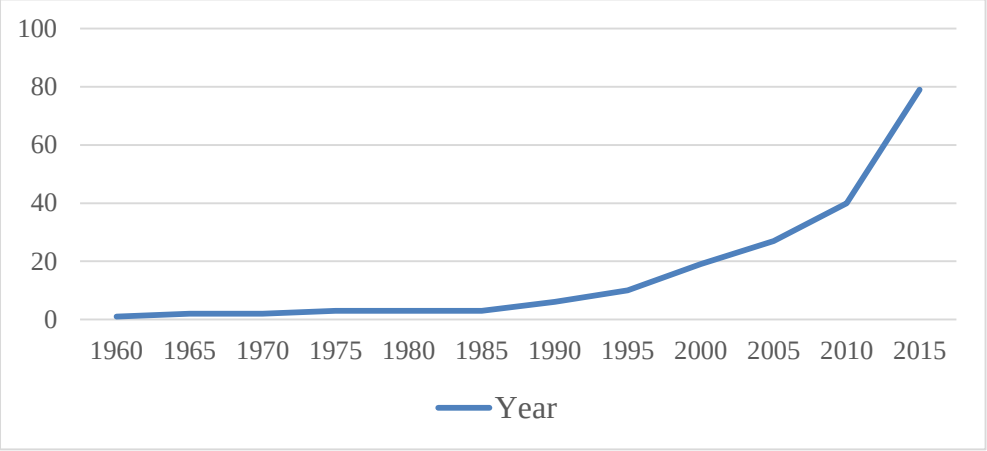
II. POLICY CONSIDERATIONS UNDERLYING DATA LOCALIZATION SURGE

Most governments are devising policies to exercise greater control over data as a response to myriad concerns associated with data being stored beyond their national jurisdiction. Most of the reasons stem from an apprehension that such states would be unable to exercise sovereignty over the

[12] A. Chander, U. P. Le, 'Breaking the Web: Data Localization vs. the Global Internet' (2014) UC Davis Legal Studies Research Paper Series 1 <http://ssrn.com/abstract=2407858> accessed 30 March 2022.

data of their citizens. Furthermore, considering the prevalent data dominance exercised by developed nations in the digital environment, particularly the USA and China, these fears are not without reason. Thus, data localization has emerged as a significant policy consideration by various nations, especially those lacking sufficient geopolitical influence, in response to such pressing concerns.[13]

Illustration I: Increase in data localization measures globally (1960 - 2015)[14]



It can be noted that a significant increase in data localization regulations has been made with the development and growth of information technology.[15] In the past few years, development in big data technologies has been a driving force resulting in increased demand for data, data control, and

[13] Emily Wu, 'Sovereignty and Data Localization' (*Harvard Kennedy School Belfer Center for Science and International Affairs*, July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> accessed 1 April 2022.

[14] United States International Trade Commission, 'Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions' (*United States International Trade Commission*, August 2017) <https://www.usitc.gov/publications/332/pub4716_0.pdf> accessed 1 April 2022.

[15] ibid.

subsequent data localization.[16]

Reliance on widening data localization policies is primarily on technical concerns associated with the free flow of data. Such factors vary from (a) Data safety, and national security including foreign surveillance; (b) Restricted access to data stored beyond national jurisdiction; (c) Concerns regarding the overuse of personal data including breach of privacy rights; (d) Inability to access data necessary for prevention and investigation of crimes by national law enforcement and security agencies; and (e) Inability to reap economic benefits from data of their nationals on account of its control and exploitation by foreign companies.[17]

At the same time, geopolitical realities and the wide global divide in terms of dominance by developed nations in the technological environment, infrastructure, and control over access is of grave concern. Value concerns associated with such data dominance by a select few have given rise to pertinent fear of a form of "neo-colonialism" in the present times.[18] Furthermore, failure in establishing privacy and data protection norms and past incidents such as the expose by Edward Snowden keeps the distrust

[16] Yanqing Hong, 'Data Localisation: Deconstructing Myths and Suggesting a Workable Model for the Future - The Cases of China and the EU' (2019) 5(17) Brussels Privacy Hub Working Paper <https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL5-N17.pdf> accessed 2 April 2022.

[17] Anirudh Burman and Upasana Sharma, 'How Would Data Localisation Benefit India?' (2021) Carnegie Endowment for International Peace Working Paper <https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf> accessed 2 April 2022.

[18] Carla Hobbs and others, 'Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry' (*European Council on Foreign Relations*, 30 July 2020) <https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/> accessed 2 April 2022.

alive.[19] Therefore, the immediate focus has shifted to controlling presently unregulated data flow by putting in place even more expansive data localization requirements. It is for these technical, value, and practical concerns that data localization as a response has been resorted to by various policymakers to strengthen data control.[20]

III. IMPLICATIONS UNDERLYING DATA LOCALIZATION POLICIES

Time and again, data localization measures are referred to by regulators and policymakers as a possible approach to ensure better privacy, data security, and infrastructural and economic development.[21] However, even if intended towards securing such ends, it is relevant to evaluate the probable impact and implications of data localization on them.

A. Privacy Concerns

The issue of privacy concerns over cross-border data transfer per se does not arise in the case of transferee nations that have established adequate privacy protection safeguards but rather with transferees which fall below such thresholds. This threshold of adequate protection is both subjective and in a

[19] Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders' (2014) 2(3) The Lawfare Research Paper Series <https://www.researchgate.net/publication/272306764_The_Growth_of_Data_Localization_Post-Snowden_Analysis_and_Recommendations_for_US_Policymakers_and_Business_Leaders > accessed 3 April 2022.

[20] Yue Wang, 'Analysis on the Justification of Cyber Data Localization Legislation' (2016) 36 J of Xi'an Jiaotong U (Social Sciences).

[21] Shamel Azmeh and Christopher Foster, 'The TIPP and The Digital Trade Agenda: Digital Industry Policy and Silicon Valley's Influence on New Trade Agreements' (2016) London School of Economics Working Paper No. 16-175, 26-27 <https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf> accessed 3 April 2022.

constant state of change. Therefore, the focus is on establishing effective frameworks to secure privacy within the nation as well as globally through technical measures such as design mechanisms in networks and digital systems and encrypting user data.[22] Therefore, data localization has a limited impact on addressing the actual problems associated with data privacy itself.[23]

The prevalent frameworks engaging bilateral mutual data transfer systems are cumbersome and impractical in the long run as noted in the case of the invalidation of the EU-US Privacy Shield.[24] Therefore, the discourse towards greater privacy protection lies in establishing a working multilateral discourse that prioritizes privacy along with responsible data transfer in the future. For instance, the Asia-Pacific Economic Cooperation (**"APEC"**) has worked towards such a solution in the form of the Cross-Border Privacy Rules (**"CBPR"**). The CBPR provides a certification framework that globally provides for the exchange of data between entities that meet the necessary accountability requirements.[25] Such frameworks provide more holistic data privacy mechanisms which are aligned with global requirements without creating excessive cost and offer the possibility of greater adoption. Similarly, the ongoing Data Free Flow with Trust (**"DFFT"**) initiative by Japan proposes a possible solution that offers an interoperable system, which targets

[22] Bret Cohen, Britanie Hall and Charlie Wood, 'Data Localisation Laws and Their Impact on Privacy, Data Security and the Global Economy' (2017) 32(1) Antitrust 107.
[23] Helena U Vrabec and others, 'Data Localisation Measures and Their Impacts on Data Science' in Roland Vogl (ed), *Research Handbook on Big Data Law* (Edward Elgar 2021).
[24] Ryan Browne, 'EU and US agree to new data-sharing pact, offering some respite for Big Tech' (*CNBC,* 25 March 2022) <https://www.cnbc.com/2022/03/25/eu-and-us-agree-new-data-transfer-pact-to-replace-privacy-shield.html#:~:text=Privacy%20Shield%2C%20an%20arrangement%20allowing,was%20invalidated%20in%20July%202020> accessed 4 April 2022.
[25] Asia Pacific Economic Cooperation, 'What is The Cross-Border Privacy Rules System' (*Asia Pacific Economic Cooperation,* October 2021) <https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system> accessed 5 April 2022.

developing trade rules for cross-border data transfer while considering the actual differing circumstances existing.[26]

India has raised concerns about the sweeping provisions of the DFFT and calls out for policy space to develop its own domestic legal framework first.[27] However, the two cardinal principles of the DFFT i.e. careful protection to be guaranteed to sensitive and personal data, and free flow of data such as industrial or medical for economic purposes, help in the establishment of a useful baseline balancing data privacy and data transfer.[28] India should take into consideration such a model which can help it develop a more symmetrical framework of data protection and data transfer, inconsonance with global economic realities.

B. Access to Data by State

Another aspect for which emphasis is cast on data localization is expeditious access of data by law enforcement agencies by doing away with the 'request' framework established under the present Mutual Legal Agreement Treaty (**"MLAT"**) regime. The fact of the matter remains that the

[26] Nigel Cory, Robert D. Atkinson and Daniel Castro, 'Principles and Policies for "Data Free Flow Trust" (*Information Technology and Innovation Foundation*, 27 May 2019) <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust> accessed 5 April 2022.

[27] Asit Ranjan Mishra, 'India Says No to Free Flow of Digital Data at G20 Meeting' (*LiveMint*, 22 Sep 2020) <https://www.livemint.com/news/india/india-says-no-to-free-flow-of-digital-data-at-g20-meeting-11600787726265.html> accessed 4 May 2022.

[28] Karthik Nachiappan, '579: The Battle Over India's Data Policy Framework: What Gives?' (*ISAS NUS*, 4 Sep 2019) <https://www.isas.nus.edu.sg/papers/579-the-battle-over-indias-data-policy-framework-what-gives/> accessed 4 May 2022.

MLAT framework is a time-consuming process[29] that lacks transparency,[30] is afflicted by differing ineffective privacy standards,[31] and tends to dilute the due process element in trials.[32] Therefore, the solution lies in introducing a new framework that addresses the lacunas posed by the MLAT regime.

Thus, emphasis should be on devising multilateral arrangements which overcome the lacunas in the present-day MLAT regime. For instance, the US Clarifying Lawful Overseas Use of Data Act (**"CLOUD Act"**) requires certification from the competent authority based on the privacy and civil liberties standards and safeguards maintained by the transferee nation.[33] It further requires an assessment of the overall terms of the agreement to evaluate if it meets the standards under the CLOUD Act.

C. Safety of Data

Safety and security of data is a factor no longer dependent on the physical location of data but rather on the policy framework and security measures of the entities dealing with it. This becomes even more relevant considering the use of data by large global corporations across multiple jurisdictions. Storing large volumes of data at one physical location or with a

---

[29] Bedavyasa Mohanty and Madhulika Srikumar, *Hitting Refresh: Making India-US Data Sharing Work* (Observer Research Foundation Special Report No 39, 2017).

[30] Amber Sinha and others, 'Cross-Border Data Sharing and India' (*The Centre for Internet and Society,* September 2018) <https://cis-india.org/internet-governance/files/mlat-report> accessed 5 April 2022.

[31] Sarah Cortes, 'MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance' (2015) 22(1) Rich JL & Tech 1.

[32] Robert J. Currie, 'Human Rights and International Mutual Legal Assistance: Resolving the Tension' (2000) 11(2) CLF15.

[33] Emily Wu, 'Sovereignty and Data Localization' (*Harvard Kennedy School Belfer Center for Science and International Affairs*, July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> accessed 5 April 2022.

centralized data storage center would enable the possibility of a catastrophic breach.[34] Therefore, this issue of safety and security of data is not based on the location of data per se but on technical safeguards and cyber security measures.[35]

On the other hand, certain sectors are heavily reliant on the free flow of data to ensure better security. One such instance is the payment systems being used globally which require data not only to improve and update the payment networks but also to detect fraud, notify it, and prevent it in the future. Therefore, in such cases where the flow of data is disrupted and restricted within territories, the ability of the system to detect instances of fraudulent activity would be limited and would expose such payment systems to risk.[36]

D. Economic Considerations

Considering the interconnected nature of the global economy, ill-conceived data localization policies can lead to creating substantial data storage and processing costs. These actual costs can severely impact the economy in general and certain digitally reliant sectors in particular. Similarly, sectors such as e-commerce, manufacturing, exports, finance, logistics, and service providers, which require secure, continuous access to cross-border data would be unable to function efficiently. Such data localization not only disrupts economic growth and the flow of business but also acts as a deterrent to further innovation which is based on the borderless nature of the internet

[34] cf Vrabec (n 23).
[35] ibid.
[36] Rajat Kathuria and others, 'Economic Implications of Cross-Border Data Flows' (*Indian Council for Research on International Economic Relations*, November 2019) <https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf> accessed 6 April 2022.

and reliant on the free flow of data. The Leviathan Security Group estimated the burden of data localization could result in the rise of costs for such entities by 30-60%.[37] Such policies create tendencies of raising barriers and limiting possibilities, especially for small-scale entities and new players in a sector.

IV. DATA LOCALIZATION FRAMEWORK IN INDIA

In the past few years, India has taken significant steps by amending and introducing laws toward a wider data localization policy. Most significant developments in this regard have been made in the case of the corporate, finance, insurance, banking, and electric sector. In 2018, the Reserve Bank of India required certain organizations to store and maintain payment data in India.[38] Similarly, the IRDAI (Maintenance of Insurance Records) Regulation, 2015[39] requires insurers to store and maintain data within India.[40] Furthermore, Section 94 read with Section 88 and 92 of the Companies Act, 2013[41] requires financial information to be maintained at the registered office of the company by such specified companies.

The Personal Data Protection Bill 2019 (**"PDP Bill"**)[42] has laid down further requirements for data localization of sensitive personal data and critical personal data. In December 2021, after two years of deliberation, the Joint Parliamentary Committee (**"JPC"**) laid down its report on the PDP Bill. The

---

[37] Brendan O'Connor, 'Quantifying the cost of forced localization' (*Leviathan Security Group*, 24 June 2015) <https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization> accessed 6 April 2022.
[38] Reserve Bank of India Dir 2017-18/153, para 2(i).
[39] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulation 2015.
[40] ibid para 3(9).
[41] The Companies Act 2013, ss 88 and 92.
[42] The Personal Data Protection Bill 2019 (373 of 2019).

JPC has emphasized the importance of storing data within India and mirroring copies stored outside India in light of growing national and security concerns. The report has stressed developing policy to eventually localize all forms of data within India. Therefore, it has focused the attention on the need for developing greater data storage infrastructure, while supporting and assisting businesses within India and ensuring ease of doing business with India.[43]

V. IMPACTS OF WIDENING DATA LOCALIZATION

The impact and practical implications of data localization measures in India can be assessed from three perspectives.

A. Economic Impact

Ultimately, it is critical to evaluate the cost-benefit and overall effect of data localization on the economic growth of India. In 2014, European Centre for International Political Economy provided that a mandatory localization policy could negatively impact India's GDP by 0.8%.[44] In terms of the welfare cost, India would be losing 11% of the monthly salary per worker.[45] Another study estimates investment losses in India to amount to US $18bn and the welfare losses to US $2.4bn by 2025.[46]

---

[43] Joint Parliamentary Committee, *Report of the Joint Committee on The Personal Data Protection Bill, 2019* (16 December 2021) 8-10.

[44] M Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (*European Centre for International Political Economy*, May 2014) <https://ecipe.org/publications/dataloc/> accessed 7 April 2022.

[45] ibid.

[46] CUTS International, 'Data Localisation: India's Double Edged Sword?' (*CUTS International*, Jaipur 2020) <https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf> accessed 7 April 2022.

The lack of infrastructure to support sweeping data localization policies would force additional costs towards hardware investments either by improving existing data centers or by investing in cloud service providers. In terms of data center infrastructure, India accounts only for 1.2 percent globally and 5.23 percent in the Asia-Pacific region.[47] The Asia Cloud Computing Association in its Cloud Readiness Index has ranked India at 10 out of the 14 Asian countries it studied and a score of 56.7 out of 100.[48] It will also have a critical impact on investment which is essential for any digital development, particularly digital infrastructure which is presently targeting to attract significant FDI. Presently, on account of the high cloud service cost,[49] lack of data centers, and associated infrastructure, the possibility of India hosting such significant quantities of data would prove uneconomical.[50]

B. Privacy and Civil Liberties

The issue of privacy concerns over citizens' data is dependent on developing an effective data protection framework not only against foreign nations and entities but also the state and domestic entities. India has been lagging behind its global counterparts on this front despite the landmark pronouncement of the Hon'ble Supreme Court in *Puttaswamy v. Union of*

---

[47] Internet and Mobile Association of India, 'Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure' (*IAMAI*, May 2016) <https://www.medianama.com/wp-content/uploads/iamai-make-in-india-data-center-report-india.pdf> accessed 8 April 2022.

[48] Asia Cloud Computing Association, 'Cloud Readiness Index' (*Asia Cloud Computing Association*, 2020) <https://www.digitalcentre.technology/wp-content/uploads/2020/06/CRI2020_ACCA_Final.pdf> accessed 8 April 2022.

[49] Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, 'The Localisation Gambit-Unpacking Policy Measures for Sovereign Control of Data in India' (*The Centre for Internet and Society*, March 2019) <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf> accessed 8 April 2022.

[50] ibid.

India,[51] recognizing privacy as a fundamental right. Therefore, the need of the hour is not sweeping data localization but rather a strong workable privacy framework in harmony with global standards and safeguards.

Furthermore, sweeping measures of mandatory data localization would have to stand the test of being proportionate, reasonable, just, and fair as laid down by the Puttaswamy judgment.[52] It is on these thresholds that mandatory data localization will not hold ground in the face of more proportionate alternatives. At the same time, it can be reasonably apprehended that such measures could be counter-intuitive and premature in guaranteeing any form of privacy, especially against the state. Such data localization can encourage wide-scale surveillance and intrusive measures by local governments which in many ways can cause irreparable damage to civil liberties.[53]

C. Access to Data by the State

Accessing information stored beyond the jurisdiction of the state is a compelling challenge for the state. Therefore, it appears that localization would aid law enforcement agencies to access data and implement local laws more effectively. However, this too has its fair challenges. Modern technologies such as encryption techniques would require state agencies to invoke more comprehensive legal processes to overcome such issues. Under such localization requirements, smaller entities might exit the market but

[51] *Justice K.S. Puttaswamy and Anr. v. Union of India and Others*, (2017) 10 SCC 1.
[52] ibid.
[53] Gautam Bhatia, 'Making the Internet Disappear' (*The Hindu*, 18 October 2017) <https://www.thehindu.com/opinion/lead/making-the-internet-disappear/article19877770.ece> accessed 10 April 2022.

larger corporations such as Whatsapp, Twitter, Google, and Facebook, are more likely to continue and are harder to negotiate with.[54] A viable solution for the present situation, particularly concerning US-based entities, would be to enter into an agreement under the CLOUD Act that would help India mitigate the MLAT issues and still gain access to Indian data held by US firms. In the longer run, limited localization mandates which are targeted for specific purposes might prove more conducive for India.

VI. THE GLOBAL INTERPLAY WITH DATA LOCALIZATION

The current global dialogue on data localization is strongly impacted by the prevalent North-South geopolitical divide. The present data framework is focused on harvesting data from the South to be processed, stored, and utilized by the North. This pattern has led to a surge in interventions by the developing countries calling out the hegemony of the North over digital intelligence and reclaiming control over their data by supporting indigenous platforms.[55] India has been developing its stance along these lines in recent years with payment data local storage mandate, digital taxation on foreign businesses and platforms, stricter regulations, and supervision of significant social media companies.[56]

---

[54] Justice BN Srikrishna, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (*Ministry of Electronics and Information Technology*, 27 July 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 10 April 2022.

[55] cf CUTS International (n 46).

[56] Mark Linscott and Anand Raghuraman, 'Atlantic Council India's Digital Policies are Putting US Tech in a Bind' (*Atlantic Council*, 10 August 2021) <https://www.atlanticcouncil.org/blogs/new-atlanticist/indias-digital-policies-are-putting-us-tech-in-a-bind/> accessed 11 April 2022.

Therefore, global data localization is taking up two patterns, firstly, hard data localization is enforced by China, Russia, Indonesia, and Nigeria, through which such countries prohibit/restrict the cross-border flow of data outside the national territory.[57] Secondly, countries allow the regulated and conditional flow of data which may or may not include local storage of data. These conditions vary depending on legal, regulatory, certification requirements, etc.[58] Most nations have taken steps anywhere between these two approaches with varying degrees of control over data transfer, nature of the data, applicability, and enforcement measures. In this regard, most data localization steps have been with regards to specific sectors targeting critical and sensitive data such as health records in Australia, cloud service providers working for the department of defense in the United States, and data to ensure accountability in the government system in Canada, etc.[59]

On the other hand, several regions/countries have identified more frameworks focused on developing robust cross-border data transfer while utilizing data localization policies where necessary. The European Union's GDPR has been one of the most significant data protection frameworks. It provides for the free flow of personal data to regions/entities that meet the 'adequate level of protection' requirement.[60] In terms of non-personal data, the EU Regulation (EU) 2018/1807 facilitates the free flow of data by

---

[57] A Segal, 'Year in Review: Chinese Cyber Sovereignty in Action' (*Council on Foreign Relations*, 4 December 2017) <https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action> accessed 11 April 2022.

[58] cf Kathuria (n 36).

[59] cf Basu (n 49).

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 45.

prohibiting member states from localizing such data which is not under the scope of the GDPR.[61] It limits the conditions for local storage on the ground public security and after communicating such localization to the European Commission.[62] Therefore, the focus is on demanding and maintaining adequate data protection standards to ensure a safe and accountable free flow of data.

Similarly, Singapore under the Personal Data Protection Act, 2012 (**"PDPA"**) provides for cross-border transfer of personal data only if the prescribed standards and requirements under the PDPA are ensured by the organization.[63] The PDPA creates a dual obligation on the organization to comply with the legally enforceable data protection mandates while it is in possession of such personal data and at the same time to ensure that the recipient maintains standards similar to the PDPA in safeguarding such data.[64]

To overcome the differences in domestic privacy legislation, APEC has developed the CBPR. The CBPR works as an enforceable certification system in which companies can join voluntarily to comply with globally recognized standards to ensure data privacy and protection.[65] Furthermore, both the EU under the Binding Corporate Rules System and APEC CBPR mandate such companies to establish processes for independent review to ensure necessary protection in case of data transfer.[66] The EU scrutinizes

[61] Regulation (EU) 2018/1807 of the European Parliament and of Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.
[62] ibid.
[63] Personal Data Protection Act 2012, s 26(1).
[64] Personal Data Protection Regulations 2021, reg 10.
[65] Asia Pacific Economic Cooperation (n 25).
[66] United Nations Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (*United Nations*

contracts under which data is primarily transferred to assess whether the wording of the contract ensures sufficient data protection. The EU also provides individuals the opportunity to consent to the transfer of their data to a foreign country/entity as a mandatory condition.[67] However, this form of consent might prove ineffective, illusionary, and impractical under various circumstances. Therefore, best practices evolving to facilitate data transfer focus on combining elements of different approaches to mitigate many of the concerns driving data localization practices.

VII. CONCLUSION AND RECOMMENDATIONS

The most pertinent issue at present surrounding data localization is the lack of a global consensus in terms of the future of data sharing, privacy, and protection. Therefore, in a global arena greater initiative needs to be undertaken to facilitate key policy options. These policy considerations involve:

- Constant dialogue on different aspects of data control and protection, while targeting greater transparency and involvement of developing nations and stakeholders. Such engagement is critical in identifying a workable balance between data protection, innovation, and digital economic growth.
- Move away from piecemeal sector-specific legislation and develop broad, comprehensive data privacy and regulatory frameworks. For instance, cybercrime and data protection should be discussed under broader legal frameworks such as the Budapest Convention on

Conference on Trade and Development, April 2016) <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> accessed 12 April 2022.

[67] Regulation (EU) 2016/679 (n 60), art 6.

Cybercrime which requires revision and improvement and a possible protocol, to become truly effective.

- Efforts have to be made to imbibe common principles and best practices to move towards an interoperable system. Such interoperability signifies developing legal frameworks addressing concerns such as data transfer, privacy, cybersecurity, and other issues through a similar framework guaranteeing an adequate level of protection. Digital interoperability should introduce greater regulatory interoperability which can be attained through consensus, agreement, and, recognition of global principles and certification standards for instance under the APEC CBPR framework.
- On the domestic front, the focus has to be directed towards establishing functioning regulatory bodies and robust enforcement mechanisms to address appropriately data breaches and privacy violations.
- To actively deliberate on data transfer and localization issues in light of:
    - Data transfer exceptions such as law enforcement requests, emergencies, in furtherance of contractual obligations, etc. The initiative should be taken by major developed countries to improve existing frameworks such as the MLATs and to facilitate greater assistance under existing domestic laws such as the United States CLOUD Act.
    - Establish a working model of a comprehensive evaluation to identify jurisdictions that provide an adequate level of data protection standards.

  - Procedure to evaluate the corporate policy and rules within corporate entities engaging in different capacities with data and data transfer.
  - Lay down necessary accountability standards for foreign entities in case of any breach.
- To facilitate developing nations in their capacity-building efforts towards establishing data protection frameworks and also their effective implementation.

Since India stands at the cusp of developing its data policy, in addition to the above-stated aspects, it is pertinent for it to engage with the following considerations to identify a workable balance in the coming future:

- Data localization measures do not provide India the access to data stored beyond the national jurisdiction and therefore they do not resolve jurisdictional conflicts or further jurisdictional claims. Thus, India would have to initiate opening up channels of negotiation under key instruments such as the European Union's e-Evidence Directive, US CLOUD Act, etc. This is particularly important in dealing with foreign entities bound by such instruments. India should leverage its present stance to exercise greater pressure on countries that rely on such data and resolve deadlocks in the present data-sharing framework. It will also enable India to stress for more workable bilateral/multilateral agreements that ensure time-bound sharing of data with Indian law enforcement agencies in light of Indian laws.

- To evaluate and identify the most critical and beneficial data categories for local data storage instead of applying sweeping data storage mandates.
- To research and identify structured, systematic, and phased localization mandates through transparent engagement with important stakeholders.
- India should also work towards developing its framework for data sharing and conditional mandates to maintain the privacy and security of data. This will ensure that data of Indian citizens are treated with the necessary precaution and safety standards and also uplift India's position globally.
- In light of possible threats to fiber optic cables and cyberattacks, India needs to align strong defense, and initiate dialogue and alliances with countries holding strategic positions.
- To strategically plan and develop robust internet infrastructure to meet requirements of future data localization policies, as and when necessary.

Strategically, it would be extremely onerous to the digital economy for India to introduce sweeping data localization mandates at this point. Therefore, the global patterns also encourage India to redirect its effort towards the development of a legal framework that facilitates certainty and stability in cross-border data transfer. However, this provides only an important starting point for the Indian government to evaluate data localization as a policy consideration in light of the present circumstances and to assess its viability to achieve broader future objectives.