SUPREMO AMICUS

VOLUME 25 | AUGUST, 2021 ISSN 2456-9704

PRIVACY AND INTERMEDIARY LIABILITY IN DATA LOCALISATION: THE DEVIL IS IN THE DETAILS

By Anam Danish
From Jamia Millia Islamia

ABSTRACT

Governments all over the world seem anxious to gain control over the world wide web and in their desperation to do so appear to be breaking it apart. South Korea, for instance, is determined to keep its mapping data within its borders. The Australian government remains cautious about their health data leaving the country. Vietnam maintains a copy of all its data. Nations across the world continue to erect 'Schengen Zones' for their data ultimately sabotaging the possibility of global facilities. Increasing requirements for data localization threaten major new advances in information technology which is not just limited to cloud computing but also threatens the promise of big data and the Internet of Things. Localization of data undermines social, economic and civil rights by eroding the ability of individuals to gain access to knowledge and international markets, by giving governments greater control of local information[1]

INTRODUCTION

The paranoia of foreign surveillance has led governments across the world to take drastic measures to keep data from leaving their respective borders. Recklessly giving access to data to foreign agencies jeopardizes privacy and security measures.

'Data Localization' impedes data from being transferred across a nation's borders. Countries either set up regulations that completely halt the transfer of information or require lengthy transfer procedures that operate on prior consent.

Essentially, countries seem to be setting up national barriers curtailing the flow of their data, which does away with the whole purpose of setting up the worldwide web. Data localisation dramatically alters the fundamental architecture of the world wide web, threatening global services. For a state trying to localize their data, this would mean building a physical local base in every domain in which they operate, increasing the financial burden of both internet providers and consumers. Data localisation continues to be a debated issue in India especially after the idea of localising the payment and personal data sector was considered.

It is imperative to understand that this is not an issue which can be understood in isolation. Data localisation has to be viewed with regard to the political and economic expansion of a state.

Part I of the essay describes the data localization measures in place or proposed in India. Part II attempts to look at localization globally and its impact on the Indian economy. Part III of the essay argues that data localization undermines privacy and security and attempts to analyse the depths of intermediary liability.

[1]Director, California International Law Centre, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.DYale Law School.

I. TRACING THE HISTORY OF DATA LOCALIZATION: INDIA

The Ministry of Communication and Technology in April of 2011 published rules implementing specific provisions of the IT Act, 2000. The IT Act limited the transfer of *"sensitive personal data or information"* when *"necessary"* or on consent from the individual. Rule 7 read: *A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.*[2] The ambit of the term *"necessary"* was so broad that it became impossible to navigate. The rule also failed to mention how one could obtain *"consent"* in order for the data to be transferred. The rule in certain cases was satisfied with written consent by email and fax. This consent in *"writing"* too was incredibly ambiguous and left space for personal interpretation. European laws, for instance, require consent in cases of data collection but not specifically for transfer abroad. Special consent for the transfer of data conveyed that this data is somehow less safe and hence the extra steps.

A consent requirement was set up for the transfer of data to India from the United States after a significant outcry on outsourcing to India. Indian law too accomplished this goal by requiring American companies to obtain the prior consent of individuals willing to transfer their information to India.

The Ministry of Communication and Technology in August of 2011 clarified that these rules were directed at companies located in India gathering local data.

Digital Information Security in Healthcare Act, 2018[3] was published on 21st March 2018, empowered the proposed National Electronic Health Authority to impose localisation requirements with respect to digital health data.[4] The Reserve Bank of India issued a directive on 6 April 2018 imposing rigorous data localisation stipulations on all individuals in the Indian payments ecosystem. This directive made it mandatory for all payment system providers, suppliers and intermediaries to store payment-related data in its entirety in India.[5]The requirement also extends to intermediaries hired on a contractual basis who possess payment-related data.

Justice B.N Srikrishna was assigned with the task of coming up with a new data protection

[2]The Information Technology Act, 2000 (Act 21 of 2000)

[3]Overview: Digital Information Security in Healthcare Act (#DISHA) available at https://www.ikigailaw.com/overview-digital-information-security-in-healthcare-act-disha/ (Last Modified 7 May, 2018)

[4]Notice by Ministry of Health & Family welfare, Government of India (21st March 2018) available at https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf

[5]Guidelines on Regulation of Payment Aggregators and Payment Gateways (Updated as on November 17, 2020) available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0

framework for India *'Srikrishna Committee, 2018'*. The committee submitted the Personal Data Protection Bill to the government on 27th July 2018, with detailed recommendations.[6] The committee propounded that a copy of Indian personal data should be stored in India. Section 97(7)[7] of this draft bill empowers the government to bring the provisions of the act in force at any time of their choosing or not bring into force at all. These developments collectively pushed towards localisation an idea which was viewed by the public with caution.

The National Security Council in 2014 considered hosting all Indian-based data on Indian-based servers. While this hasn't been brought into effect localisation policies already seem to exist in several sectors.

- **Data protection under the IT Act, 2000:** The IT Act primarily provides data protection provisions. Section 43A of the act awards compensation in case of failure of maintaining reasonable security practices for *"sensitive personal data"*. The rules issued in 2011 defined *"sensitive personal data"* and laid out norms for the storage and collection of such data. Transfer of data was allowed as long as the other party could continue to ensure the *"same level of data protection"*.[8] However, the law failed to establish a procedure to determine an entity's *"same level of data protection"*.[9] Leaving compliance with the said rules, questionable.
- **Government Data:** The Public Records Act, 1993 forbids the transfer of public data out of Indian territory without prior consent from the Central Government, unless the said transfer is being made for official purposes. The 'Megh Raj' initiative which harnesses the use of cloud computing, also requires the localisation of government data.[10]
- **Sector-Based Desideratum:** The government bars telecom service providers from transferring user or accounting information abroad through license agreements, exceptions are provided only in cases of international roaming purposes.

RESERVE BANK OF INDIA

Despite multiple instances of acknowledgements from the financial sector about the need for improvements in regulatory processes related to data localisation. The RBI's *'localisation directive'* was brought forth without any prior discussion or public discourse.[11] RBI's Statement on Development and Regulatory Policies, which was succeeded by the localisation directive concerned itself with the need for adopting the finest global safety and security procedures, to avoid data breaches. But the following questions remained unanswered. Were there any instances of non-compliance by data entities? Were there any security breaches? Was there trouble in managing lapses in data security? In the absence of such explanations, the said

[6]Key Highlights From Srikrishna Committee Report on Data Protection available at https://www.thequint.com/news/india/key-highlights-from-srikrishna-committee-report-on-data-protection (Last Modified 27, July 2018)

[7]The Information Technology Act, 2000 (Act 21 of 2000)

[8]RK Dewan and Co "Personal Data Protection Laws in India" https://www.lexology.com/library/detail.aspx?g=081 97ebe-aeb4-41d6-a855-ce57a313ea6d (Last Modified May 13 2020)

[9]Sinha & Hickok, 2018

[10]NIC available at https://cloud.gov.in/about.php

[11]RBI issues clarifications on data localisation circular available at https://www.business-standard.com/article/news-ani/rbi-issues-clarifications-on-data-localisation-circular-119062700235_1.html (Last Modified June 27, 2019)

directives lacked sufficient reasoning to support the RBI's claims.

II. THE GLOBAL PERSPECTIVE

According to the Digital Trade Estimates index created by the European Centre for International Political Economy (ECIPE)[12], 64 countries from 1961 to 2016, introduced data localisation requirements. Among them 42% imposed a list of conditions to be fulfilled before the transfer of data; 25% imposed storage processing requirements; 33% imposed a complete ban on transfers outside the jurisdiction.[13] Russia, Indonesia, China and Vietnam have adopted relatively broad localisation requirements. Australia, Germany and France, on the other hand, have stuck to a sectoral based approach (Cory, 2017). Most countries seem to use data protection and prevention of foreign surveillance as a basis for their localisation decisions.

ECONOMIC IMPACT: INDIA

Localisation may result in serious violations of the rights granted under Article 19(1)(g)[14] and due consideration should be paid while drafting localisation policies.

A study conducted by the European Centre for International Political Economy quantified the losses from localisation.[15]

Imposing economy-wide data localisation could reduce the Indian GDP by 0.8% and domestic investments by 1.4%.[16] The study further looked at welfare costs on a worker basis and found, in India, the loss per worker would be equivalent to 11% of the average monthly salary. It was concluded that *"any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy"*[17] The negative impact was the highest on financial services, communication services and data-intensive industries since this sector is increasingly dependent on data inputs. Restricting the free flow of data would ultimately mean a backward shift in an economy's production structure.

III. PRIMARY CONCERNS RELATED TO LOCALISATION

- **PRIVACY**

The Supreme Court in 2017 recognised the right to privacy as an integral element of numerous fundamental rights ranging from Articles 14-18, Article 19 (1) (a) and Article 21 under the Indian Constitution (Puttaswamy v. Union of India, 2017).[18] However, the court noted that the right to privacy was not an absolute right and it could be restricted on certain grounds. The consensus of the judgement is that the right to privacy must satisfy the requirement of being *"just and reasonable."*

The judges also settled on additional tests to analyse privacy infractions. The tests include

[12]ECIPE available at https://ecipe.org/tag/data-localisation/

[13]Martina F. Ferracane, Janez Kren, Erik van der Marel "The cost of data protectionism" https://voxeu.org/article/cost-data-protectionism (Last Modified 25 October 2018)

[14]Article 19(1)(g) in The Constitution Of India

[15]ECIPE available at https://ecipe.org/tag/data-localisation/

[16]ECIPE available at https://ecipe.org/tag/data-localisation/

[17]Reconsider imposition of data localisation: IAMAI report availble at https://www.outlookindia.com/newsscroll/reconsider-imposition-of-data-localisation-iamai-report/1627110 (Last Modified 25 September 2019)

[18]Justice K.S.Puttaswamy(Retd) ... vs Union Of India And Ors. on 24 August, 2017, Citation: Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

The existence of a law, the law must seek to achieve a legitimate purpose for the state, there must be a proportionality between the object and the means to adopt them.[19]

Apodictically, localisation infringes on the autonomy of individuals with respect to their private information, which is why these measures need to satisfy the Puttaswamy tests.

- **Centralising Information:** Localising information like this without adequate infrastructure and technical capacity may pave the way for hackers to target centres owing to the quantity and size of user information they store. Splitting data into groups as and when required by law, could lead to derelictions. Mirroring too leaves a lot of room for colossal errors. Localisation costs also reduce the ability of entities to store data securely. Unless there exist appropriate technical frameworks to preserve privacy locally and globally, localisation does not seem viable.
- **Foreign Surveillance:** Data stored on computer systems of multiple countries including India was accessed through tampered hardware and by injecting malware into the systems and getting physical access through entities operating in India.[20] In order to implement localisation measures, we would need to develop the capacity to manufacture hardware locally, simultaneously monitoring the import of hardware and focus on increasing network security.
- **Civil Liberties:** Localisation of data would mean a substantial increase in government interference and surveillance, compromising the internet's ability to be a *"free space" r*estricting the freedom of speech and expression ostensibly.

But, instead of viewing the issue as a barter between civil liberties and economic development a more constructive approach would be to try and balance the two, by actively protecting civil liberties through localisation.[21]

- **INTERMEDIARY LIABILITY**

'Intermediary' has been defined in Section 2(w) of the Information Technology Act, 2000 as *"any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, web-housing service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes".*[22] Ordinarily, intermediaries facilitate or act as a medium to use the internet. The definition extends to cyber cafes and is not limited to online intermediaries. The services they provide

[19]Bhandari, Vrinda; Kak, Amba; Parsheera, Smriti; Rahman, Faiza "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict" available at https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1

[20]End surveillance of foreign leaders of friendly nations: Obama available at https://www.business-standard.com/article/pti-stories/end-surveillance-of-foreign-leaders-of-friendly-nations-obama-114011701394_1.html (Last Modified at January 17, 2014)

[21]Rishab Bailey and Smriti Parsheera "Data localisation in India: Questioning the means and ends" availble at https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf

[22] Software Freedom Law Center "Intermediaries, users and the law – Analysing intermediary liability and the IT Rules" availble at https://sflc.in/sites/default/files/wp-content/uploads/2012/07/eBook-IT-Rules.pdf

range from collecting information, facilitating communication, assisting information exchange, providing internet access, hosting content and so on. Which makes internet service providers, social media platforms, cyber cafes, search engines all intermediaries.

Section 79 of the Act grants conditional immunity to intermediaries from liability in relation to third party activities.

Section 79(1) grants conditional immunity to intermediaries with regard to data, communication links and information of third parties, subject to **79(2)** and **(3)** of the Act.

Section 79(2) covers activities of technical, passive and automatic nature. This section only applies when intermediaries had no knowledge or control over the kind of information being stored. Additionally, **79(3)** has a *'takedown process'* for cases where the intermediary gains knowledge of unlawful content.

In **Shreya Singhal vs. UOI**, the Supreme Court read down Section **79(3)(b)** to mean that an *"intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19 (2) are going to be committed then fails to expeditiously remove or disable access to such material"*.[23] Implying that the intermediary cannot exercise their discretion as to the removal of materials. Moreover, the intermediary is not required to provide a reason for rejecting or accepting a takedown notice. The whole process is obscure and no guidelines are available for recourse if the intermediary suspects a notice to be frivolous.

Palpably, the current intermediary liability guidelines provide a very basic structure for intermediaries, which extend from providing notices to users, warning users of violations and preventing illegal activities on their platforms. Most intermediaries have in place their own set of privacy policies, usually, these policies are a mixture of local legal requirements and personal perception of the platform. Sometimes, intermediaries take harsh punitive actions which tend to vary from one platform to another based on their policies. Lack of clarity in such cases makes it difficult for users to understand why their content was flagged or taken down. This combined with the lack of transparency may lead to censorship issues. What we need are guidelines that focus on transparency and accountability for intermediaries.

Moderation systems, for instance, users need a clear path to raise complaints and appeals. In addition to this intermediaries should be required to produce reports periodically, revealing their moderation practices. In the meantime, attention should be paid by the state, to the policies that intermediaries implement ensuring that privacy-enhancing technologies are included by design.

Primary Issues with Amendments: IT Rules

- The Ministry of Electronics and Information Technology's view of looking at IT rules from the *Fake News* perspective is purblind and will have catastrophic consequences.
- Proactive censorship will have an inordinate impact on free speech.
- Section 79 is an exemption section, limited to ensuring due diligence and nothing more.
- Traceability destroys end to end encryption.
- A specific set of regulations for intermediaries creates a barrier to market entry.

[23]Shreya Singhal vs Union of India AIR 2015 SC 1523

CONCLUSION

The claim that data localisation enhances privacy, or non-access to data to the government hampers law enforcement and that localisation increases economic benefits is problematic in multiple ways.

After careful scrutiny of these arguments, we find that introducing extensive data localisation norms, will most likely outweigh its benefits. However, localisation can become a justified measure if policies incorporate the following.

- Targeting specific issues that need refinement.
- Analysing multiple alternatives to address issues along with granular reports backing each alternative.
- Prioritising the least intrusive localisation approach.
- Ensuring that the entire process remains transparent.

These measures must be incorporated completely in a new and refined law instead of amending existing data protection laws. Until a robust analysis has been conducted, all policy directives towards localisation should be delayed. India, in the meantime, should avoid entering into any trade agreements that stifle our ability to take future decisions related to data localisation. Our aspiration to create a self-sufficient *'Digital India'* must be ultimately weighted against our stance on data localisation.

*****