II. DATA LOCALISATION AND CROSS-BORDER FLOW OF DATA: BALANCING THE INCONGRUENT DIMENSION OF BARRIERS, SAFEGUARDS AND "FREE FLOW OF DATA"

- Raj Shekhar & Aman Yuvraj Choudhary[*]

ABSTRACT

The growth in today's century has been seen to go hand in hand with the globalization of society; a phenomenon of which the Internet can be seen to be a cause and a component, as well as a reflection. Data localization often refers to those policy measures which are aimed at restricting the free flow of data by limiting the physical storage and processing of data within a given jurisdiction's boundaries. The phenomenon has started to garner a plethora of international support with many countries having adopted localization policies to combat multiple concerns over the free flow of data. However, the usage of "free flow" and "data localization" seems ambiguous owing to their antagonistic nature and has been criticized by experts citing it to be against the very spirit of the internet – connectivity without barriers. The Joint Parliamentary Committee to which the Personal Data Protection Bill, 2019 was referred has once again stirred the international debate surrounding data localization by strongly supporting its implementation. In light of these issues, this paper tries to understand the plan of action, structure and objectives of data localization by the Indian Government while simultaneously carrying out a hedonistic analysis of their overall impact. It further carries out a global comparative analysis of the existing data localization practices in other mature jurisdictions and pitches forth conducive suggestions to aid in the proper implementation of such policies without hampering the crucial element of cross-border data transfer.

[*] The authors are fourth and third-year students of B.A. LL.B. (Hons.) respectively at National University of Study and Research in Law, Ranchi. Views stated in this paper are personal.

I. INTRODUCTION

The growth in today's century has been seen to be in concert with the globalization of society; a phenomenon of which the Internet is a component, a cause, and a reflection. On account of this digitalization, the concept of data privacy has assumed a position of paramount importance in the present-day digital space. This is evident from the emphasis that governments around the world, including India, have put on developing data privacy legislations. While legislations such as the General Data Protection Regulation (**"GDPR"**)[1] have proved instrumental in acting as guiding beacons, the policymakers still don't consider it sufficient. As a result, the concept of data localisation has become a significant policy issue in many countries including India. In general parlance "Data localisation" refers to the myriad policy measures that restrict the free flow of data across geographic boundaries.

The acceptance of the premise that *"data is the new oil"* has led to the origination of data protection laws worldwide, creating a variety of legal and

[1] 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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

commercial challenges for global organizations.[2] Data localisation which effectively restricts the cross-border transfer of data is one such. The phenomenon has started to garner a plethora of international support with many countries having adopted localisation policies to combat multiple concerns over the free flow of data. However, the usage of phrases "free flow" and "data localisation" seems ambiguous owing to their antagonistic nature and has been criticized by experts citing it to be against the very spirit of the internet – connectivity without barriers. The Joint Parliamentary Committee to which the Personal Data Protection Bill, 2019[3] was referred has once again stirred the international debate surrounding data localisation by strongly supporting its implementation.

The Indian Government has stated four wide objectives behind introducing the data localisation requirements which are: (i) securing more convenient access to personal data for law enforcement, (ii) bolstering economic growth and employment, (iii) preventing foreign surveillance, and (iv) better enforcement of data protection laws.[4] However, there has been no elaboration on how such a stringent data localisation policy would lead to accomplishment of these objectives (without hampering the cross-border flow of data) which is essential to globalization and development. In light of these issues, this paper tries to understand the plan of action, structure, and

[2] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 28 April 2022.

[3] 'Joint Committee on the Personal Data Protection Bill, 2019' (*PRS Legislative Research*, 28 April 2022) <https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019> accessed 28 April 2022.

[4] Anirudh Burman and Upasana Sharma, 'How Would Data Localisation Benefit India?' (*Carnegie India*, 2021) <https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf> accessed 28 April 2022.

objectives of data localisation by the Indian Government while simultaneously carrying out a hedonistic analysis of their overall impact.

II. THE EVOLUTION OF DATA LOCALISATION: ANALYSING THE DIFFERENT APPROACHES TO DATA LOCALISATION

As previously emphasized, the "data localisation" requirements have evolved and covered a majority of countries. The number of countries with data localisation legislation has almost doubled to 62 in 2021 from 35 in 2017.[5] This stands true for the total number of data localisation policies which have also more than doubled to 144 in 2021 from 67 in 2017. Another 38 data localisation policies have been proposed or considered in countries around the world in which China (29), India (12), Russia (9), and Turkey (7) are world leaders in requiring forced localisation within their respective territorial jurisdictions.[6]

On a closer analysis of the requirements and consequently the effects, data localisation measures can be classified under three major heads. To begin, several nations prohibit the transfer of certain types of data outside of their boundaries which include, but are not limited to:

- Personal data;
- health and genomic data;

[5] Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (*Information Technology and Innovative Foundation*, 19 July 2021) <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/> accessed 28 April 2022.

[6] Rajat Kathuria and Mansi Verma, '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 2 July 2022.

- mapping and geospatial data;
- government data;
- banking, credit-reporting, financial, payment, tax, insurance, and accounting data;
- publicly-traded company-internal data;
- data related to user-generated content on social media and the Internet service platforms;
- subscriber data, and communications content and metadata for traditional telecommunications and Internet-based communication services;
- and e-commerce data.

The restriction on such data transfer and a need for its localisation is based on the nature of these data being "critically sensitive" in nature.[7] For example, the USA under its Defense Federal Acquisition Regulation Supplement[8] requires an unconditional localization of critical information for operational security and national defence. Further, Russia provides for unconditional mirroring of all personal data of Russian Citizens under Federal

[7] Rishab Bailey and Smriti Parsheera, 'Data Localisation in India: Questioning the Means and Ends' (2018) National Institute of Public Finance and Policy Working Paper No. 242, 2018 <https://macrofinance.nipfp.org.in/PDF/BP2018_Data-localisation-in-India.pdf> accessed 28 April 2022.

[8] Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018).

Law.[9] Similar is the case with other prominent countries: China,[10] Indonesia,[11] Australia,[12] EU[13] *inter alia*.

Secondly, we are witnessing instances where countries are restricting data under broad umbrella categories involving data labeled as "sensitive," "important," "core," or related to national security, which often impacts a wide range of commercial data.[14] While this development in itself is alarming, in India, a broad framework targeting non-personal data is also proposed to be introduced which shall further extend the ambit of these vague data brackets. For example, the proposed framework in India is based on a similar model. While extensive data localization plans are being chalked out, hardly any heed is being paid to define the categories of data on which such measures would be implemented.[15]

Thirdly, the emergence of de facto localisation seems to have gained pace. This type of data localisation requirement makes the transfer of data extremely complicated and cost-extensive, as a result of which firms are

[9] Federal Law Number 242 – FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation.

[10] Yuxi Wei, 'Chinese Data Localization Law: Comprehensive but Ambiguous' (*University of Washington Henry M. Jackson School of International Studies*, 7 February 2018) <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/> accessed 28 April 2022.

[11] Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation.

[12] 'My Health Records Amendment (Strengthening Privacy) Bill, 2018' *Australian Parliament* (2018) <https://www.aph.gov.au/Parliamentary_Business/bills_LEGislation/bills_Search_Results/Result?bId=r6169> accessed 2 July 2022.

[13] 'EU Data Protection Rules' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en> accessed 2 July 2022.

[14] cf Burman (n 4).

[15] Vikram Jeet Singh and Kalindhi Bhatia, 'What's Driving Data Localisation in India?' (*Mondaq*, 6 May 2020) <https://www.mondaq.com/india/data-protection/928916/what39s-driving-data-localisation-in-india-> accessed 4 May 2022.

spared no option other than storing the data locally. For example, the European Union's removal of data transfer mechanisms, failure to add new certifications and other new legal tools for data transfers, and ever-ratcheting up of restrictions and conditions for the remaining mechanisms (such as standard contractual clauses) have the potential to make GDPR the world's largest de facto localisation framework.[16] Other examples include explicit consent requirements for personal data transfers and the need to submit data transfers for opaque and ad hoc authorization.

III. INDIA'S TAKE ON DATA LOCALISATION: WHY A SUDDEN PUSH?

It is believed that the regulatory interest in data localisation has gained impetus recently, however, there existed laws almost a decade back which indirectly had the essence of data localisation. In the year 2007, when the terms of the unified telecom license agreement requirements were released, the telecom service providers of India were mandated to not transfer certain information on subscribers outside India.[17] Further, as per the Companies Act, 2013,[18] companies registered in India are to maintain their books of accounts for audit and inspection in India only. The Insurance Regulatory and

[16] Nigel Cory, Ellysse Dick, and Daniel Castro, 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade' (*Information Technology and Innovative Foundation*, 17 December 2020) <https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade> accessed 2 July 2022.
[17] 'Licensing Framework for Telecom: A Historical Overview' (*Centre for Internet & Society*) <https://cis-india.org/telecom/resources/licensing-framework-for-telecom> accessed 28 April 2022.
[18] The Companies Act, 2013 (Act 18 of 2013).

Development Authority of India mandates all original policyholder records to be maintained in India.[19]

These requirements that existed much before the ongoing push are a clear indicator that data localisation had existed before and all we are witnessing today is an aggravated plan of its implementation on an expanded plane. The most recent push in this direction has been the data localisation restrictions placed on payment data by the Reserve Bank of India (**"RBI"**) which on April 6, 2018, issued a circular mandating all payment system providers to store payment data locally, exclusively in India.[20]

These developments would surely make us question the rationale behind such data localisation rules. While no straight jacket idea is provided, several rationales are given for data localisation. In certain policies where such requirements are implemented the reasons are included in the document or rule itself. For example, in the above example where RBI mandated payment data localisation, the rationale provided was to ensure an "unfettered supervisory access" to "ensure better monitoring", and protect consumer interests. However, broadly the below-mentioned subheads constitute the rationale behind data localisation requirements:

[19] Insurance Regulatory and Development Authority of India (Minimum Information Required for Investigation and Inspection) Regulations, 2020 (F. No. IRDAI/Reg/3/169/2020).

[20] Guidelines on Storage of Payment Data, (*RBI*, 2018), <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244> accessed 2 July 2022.

A. Protection of Individual Rights

Post the Supreme Court's verdict in *Justice K.S. Puttaswamy v. Union of India*,[21] a special emphasis has been supplied on the protection of an individual's privacy. As a result, attempts are being made to build a robust data protection regime that balances legitimate concerns of the state and individual interests. The Personal Data Protection Bill was accompanied with an expert committee report which justified the need for data localisation[22] on the pretext that with the changing dynamics of cyberspace, the data of Indian citizens is being exposed to foreign surveillance and attacks. Therefore, if data is hosted abroad, an effective remedy against foreign-service providers will not be available for Indians which they may have had if the data was hosted locally.[23]

B. National Security Concerns and a Better Access for Investigatory Authorities

National Security stands as the major contention put forward time and again to justify the rigorous data localisation requirements. The justification being certain critical information (such as telephone numbers) might jeopardize state security, while other data can be vital to a country's financial well-being (like payment data). The Indian Information Technology Act of 2000[24] (**"IT Act"**) has an extraterritorial application; however, it has proven

---

[21] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[22] Padmini Ray Murray and Paul Anthony, 'Designing for Democracy: Does The Personal Data Protection Bill 2019 Champion Citizen Rights?' (*Economic and Political Weekly*, 2 June 2020) <https://www.epw.in/engage/article/designing-democracy-does-personal-data-protection> accessed 28 April 2022.
[23] Ministry of Electronics and Information Technology, 'White Paper Of The Committee Of Experts On A Data Protection Framework For India' (2017).
[24] Information Technology Act, 2000 (Act 21 of 2000).

to be ineffective. For example, there have been instances where the investigation agencies have to face a dead-end owing to the foreign nations, where the required data is stored, declining to co-operate even though letters rogatory (that are issued by courts) under mutual legal assistance treaties (**"MLAT"**) to access evidence in other jurisdictions have been presented.[25] As a result, it is believed that data localisation could help in overcoming these barriers.

C. Economic Protectionism and Promotion of Indigenous Players

The requirements of data localisation which lead to the on-soil presence of data provide an economic advantage to local firms. While it cannot be denied that there are unintentional side effects, however, the local players are usually much better equipped to tackle those. For India, this is not an unusual regulatory position. Foreign investment and exchange control restrictions in India continue to limit the use of foreign currency in specific industries and activities. Foreign engagement in certain sectors, such as multi-brand retail, is still limited. In the last two decades, there has been a movement in India to open up to more international investment and engagement. [26]

A bare perusal of the above pointers is enough to substantiate the point that data localisation could indeed be a great tool of redemption. However, a critical analysis would also uncover the fact that almost every proposal for data localisation has a combination of motives. When their primary (hidden)

---

[25] Amber Sinha, 'MLAT Report' (*Centre for Internet & Society*, 20 May 2018) <https://cis-india.org/internet-governance/files/mlat-report/view> accessed 28 April 2022.

[26] 'FDI in India: Foreign Direct Investment Opportunities Policy' (*India Brand Equity Foundation*, 1 March 2022) <https://www.ibef.org/economy/foreign-direct-investment> accessed 28 April 2022.

purpose is protectionism, national security, more control over the Internet, or any mix of these, policymakers frequently employ a "dual-use" strategy with an official and ostensibly legitimate goals, such as data privacy or cybersecurity. In certain circumstances, such as India, all of them are used. A lack of proof, openness, discussion, and involvement surrounding a data localisation plan is a clear indicator of hidden objectives.[27]

IV. DATA LOCALISATION AND BALKANIZATION OF INTERNET: INTERNET NO LONGER "FREE AND AFFORDABLE"?

Internet was envisioned to be free, unrestricted, and interoperable. The entire idea behind a global network was to create an essentially free channel for the flow of data without regard for national borders. Under such a system, the data was supposed to move from location to location quickly in the most efficient manner with or without the consent and knowledge of the user. Such a free cross-border data flow has led to the development of previously unheard technical efficiencies in storing and processing data that was previously thought to be non-existent. One of the major outcomes of this borderless data transfer can be seen in technical innovations such as cloud computing, which distributes data across multiple data centers to provide cost-effective and efficient ways where users have on-demand access to a shared pool of

[27] Usman Ahmed and Anupam Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows' (2015) *UC Davis Legal Studies Research Paper Series*, Research Paper No. 480 <http://ssrn.com/abstract=2731888> accessed 02 July 2022); Jonah Force Hill, 'A Balkanized Internet? The Uncertain Future of Global Internet Standards' (2012) Georgetown J Intl Affairs 49, 49.

processing and storage resources, while the data's real physical location(s) is mainly hidden from view.[28]

The emphasis being provided on data localisation is bound to balkanize the Internet as we know it today and lead to the fragmentation of the global network into "various distinct, idiosyncratic '(I)nternets,'" resulting in delays, inefficiencies, and higher costs.[29] The data localisation requirements imposing stringent conditions have led to a situation where the existing internet would need a significant redesign of its technical architecture to adapt to the rigorous requirements.

Data localisation requirements would further force the global service providers to develop physical infrastructure in each jurisdiction separately leading to a drastic rise in the associated costs and administrative burdens. This would significantly impact the accessibility of services to the customers who would not be in a state to bear the hiked price. Moreover, this would lead to service providers operating in a "complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights."[30] Consequently, the data localisation requirements would jeopardize the benefits individual users and businesses enjoy owing to the integration of existing globalization and the economy.

---

[28] Judith Rauhofer and Casper Bowden, 'Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud' (2013) U of Edinburgh School of L, Research Paper Series No 2013/28 1, 25 <https://ssrn.com/abstract=2283175> accessed 28 April 2022.
[29] Sascha Meinrath, 'We Can't Let the Internet Become Balkanized' (*Slate*, 2013) <https://archive.ph/jSwgF> accessed 28 April 2022.
[30] ibid.

V. DRAWBACKS OF DATA LOCALISATION: THE UNSEEN CORRIDORS OF PLACEBIC SAFETY AND DEVELOPMENT

The major thrust of arguments supporting data localisation has derived legitimacy from the supposed "safety, integrity, and security" factors that such a practice promises. However, the claims fall flat on a deeper analysis of the existing and the promised future post-data localisation. To have a better understanding, a brief analysis of the same becomes imperative.

A. Data Security

Data localisation is touted as a means to promote and enhance data security by implementing a framework to ensure the privacy and security of individual data from non-state actors.[31] However, the fact that existing data is protected through best practices and state-of-the-art technology, and local storage would have no better access to such practices and technologies than leading global companies, leads to a belief that there will be instances when such local storage would not apply the same rigor due to fewer financial resources and less available expertise. As a result of these flaws, firms may face legal responsibility and poorer customer confidence as a result of being restricted to data processing and/or storage within the boundaries of nations with inferior data security standards. This clearly reflects the fact that data localisation requirements could lead to increased risks of a breach.

[31] Patrick Ryan, Sarah Falvey and Ronak Merchant, 'When the Cloud Goes Local: The Global Problem with Data Localisation' (2013) 46 Computer 54, 54, 56.

B. Preventing Foreign Surveillance

Preventing foreign surveillance is another justification for data localisation laws, which are grounded in the belief that placing data abroad jeopardizes security and privacy. This argument has gained momentum in recent days with the world witnessing increased cyber warfare from Russia and China.[32] There exists no cogent rationale behind claiming that data localisation can effectively tackle foreign surveillance activities. For example, the Russian data localisation law provides for copies of data relating to Russian citizens to be transferred internationally and stored on servers outside Russia.[33] Further, localisation in no way prevents surveillance, as physical access to the data storage or processing facilities is not technically necessary to conduct surveillance activities.[34] In contrast, such a measure could lead to an even increased ease owing to foreign players getting an edge by recognizing and concentrating their efforts in a particular direction. Thus, the entire argument about foreign surveillance falls flat too.

C. Promotion of Domestic Economic Development

Data localisation regulations are frequently touted as a way to encourage domestic economic growth; yet, there are strong grounds to assume

---

[32] Audrey Conklin, 'Chinese Cyberattacks on NATO Countries Increase 116% since Russia's Invasion of Ukraine: Study' (*Fox Business*, March 26, 2022) <https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine> accessed 28 April 2022.

[33] Christopher Millard, 'Forced Localisation of Cloud Services: Is Privacy the Real Driver?' (2015) 2 IEEE Cloud Computing <http://ssrn.com/abstract=2605926> accessed 2 July 2022.

[34] Advaya Legal, 'Data Localisation – Protection or Protectionism?' (*The Hindu Business Line*, 8 August 2021) <https://www.thehindubusinessline.com/business-laws/data-localisation-protection-or-protectionism/article35801546.ece> accessed 28 April 2022.

that they may have negative economic consequences.[35] Any improvements in the economy would most certainly be restricted to a few local firms, data centers, and related industries, with a limited scale of new employment. Data localisation could lead to incurring of significant infrastructure, data migration, and service-related costs without benefiting from the same efficiencies or economies of scale as global businesses. There is no denying that the introduction of data localisation requirements inevitably results in increased initial and ongoing costs for users, including domestic businesses. Furthermore, services may be unavailable if the related expenses are too high and the market is too small to make them economically viable. This might make it difficult for local enterprises to grow and participate in the global digital economy, especially in emerging markets that lack the technological infrastructure that is already available online.

Due analysis of the above-stated tri-fold argument clearly points to the fact that there exist no substantial grounds on which data localisation can be pushed as a necessity. The arguments generally put forth in support of data localisation hardly stand the test of logic and are backed by nothing more than flimsy claims as demonstrated above.

VI. UNDERSTANDING PROPORTIONALITY PRINCIPLE: TAKING A CUE FROM EU AND WTO JURISPRUDENCE

When referring to proportionality in data localisation measures, under international law such as EU law, WTO jurisprudence, academic literature,

[35] Ashish Aggarwal, 'Can Data Localisation Help Protect National, Economic Interests?' (*Mint*, 7 August 2018) <https://www.livemint.com/Opinion/P9bGTw36JUx8YTK0RxKGhN/The-economic-impact-of-a-strict-data-localisation-regime.html> accessed 28 April 2022.

and various trade agreements, weightage is given to considerations such as (1) whether the measures to be enacted are likely to fulfil the objectives pursued, (2) whether there is any less restrictive measure that could be enacted, and (3) whether the measure in question stands in a reasonable relation to the intrusion it will cause.[36]

In addition to this test of proportionality, the OECD Digital Economy Paper titled, 'Data Localisation Trends and Challenges: Considerations for The Review of the Privacy Guidelines' recommends (Recommendation 6) a list of comprehensive factors to be taken into account while determining proportionality. They are:

- data sensitivity;
- the object of the processing;
- whether, and the extent to which, data localisation measure effectively achieves the goals for which it was introduced;
- availability of any less restrictive measures;
- implications of the measures: international, national, direct, indirect etc.;
- evidence of intent (wherever possible to establish);
- and the implications likely to arise if also other countries adopt the same measure ('scalability' as a consideration in the assessment of proportionality).

With regards to data sensitivity, paragraph 18 of the OECD Privacy Guidelines lays down that there must be proportionality between the

[36] Dan Svantesson, 'Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines' No. 301 OECD Digital Economy Papers OECD Publishing, Paris <https://doi.org/10.1787/7fbaed62-en> accessed 28 April 2022.

restrictions (on cross-border flow of personal data) and the risk that flow of data represents. Such proportionality must be achieved by factoring in data sensitivity and purpose. Same idea shall find resonance in the Indian legislative landscape.

As regards to the object of the processing, evidence must be garnered to come to a conclusion as to whether the measures so opted for fulfilling the objects required to be fulfilled. Evidence is of key importance here.

In assessing proportionality and if there are any less restrictive measures that could be enacted, the assessor may fruitfully venture beyond domestic considerations and also take into account international consequences and implications, direct and indirect. There would be unwarranted friction where domestic data policy decisions are made without due considerations to the international policy trends. Path of minimal resistance may be preferred while making such legislative decisions so there is in turn minimal friction with the international community while keeping the national interests at high priority.

Another factor that should be considered is the scalability of the measure. That is to say that it must be considered that what would be the effect if multiple countries adopt the same mechanisms.[37] In assessing proportionality, it would be consequential to know that whether many countries already have or would adopt similar measures. If so, such large-scale adoption may point towards legitimacy of such measure. Adding factor of

[37] D Svantesson, 'Internet & Jurisdiction Global Status Report 2019' (*Internet & Jurisdiction Policy Network*, 2019) <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf> accessed April 28 2022.

scalability into proportionality assessment would level the playing field between developed and developing countries.

Significant weightage is given to state practice in international law[38] which gives an impetus to countries to engage in universal and scalable measures. Large scale adoption, for one, points to legitimacy. The OECD digital economy paper, further goes to recommend that the proportionality test must, as an additional factor, be equipped to evaluate justifications attached to localisation measures.[39] It must be able to consider what is behind the benign label of data security and localisation.

It is pertinent to note Dr Christopher Kuner's (A law professor and a leading lawyer in Brussels, Belgium, specializing in EU and global data protection and privacy laws) arguments on data nationalism which deem it synonymous with data localisation.[40] According to him, in proportionality, both objective and subjective standards should be applied. While conceding that subjective standards are difficult to work with, the paper recommends a subjective test to look at the relevant actor's interest, whether it is a legitimate interest towards localisation and protection or intended towards privacy and human rights violations. A method of making such distinction is also suggested: to look at whether the country has definite structure of data privacy that is running parallel at both international and national levels. If there is a measure restricting foreign policy violation, then there should be a

[38] Statute of the International Court of Justice (adopted on 17 December 1963, entered into force on 31 August 1965) 33 UNTS 993 art 38(1)(b).
[39] Alpha Partners, 'Update on Data Protection Law - Privacy Protection – India' (*Mondaq*, January 3 2022) <https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law> accessed April 29 2022.
[40] Christopher Kuner, 'Data Nationalism and Its Discontents' (2014) 64 Emory L J, 2089.

concomitant domestic restriction. If not so, it can be assumed that such a restriction is favouring the government in power rather than the citizens.

The above-mentioned seven-pronged test clearly highlights the fact that proportionality in terms of the application of measures is given due weightage in mature jurisdictions. However, it is striking to note that even Indian jurisprudence has a similar test which shall be elaborated on in detail in the paragraphs that follow.

VII. THE INDIGENOUS "PROPORTIONALITY TEST": A PROBABLE SOLUTION?

The Doctrine of Proportionality is a constitutional doctrine that courts use to resolve conflicts and achieve balance when competing rights exist. There have been several decisions around the world in which courts have invoked this doctrine and resolved the conflict by holding that rights and limitations must be interpreted harmoniously to facilitate coexistence.[41] It is critical to ensure that any proposed framework for cross-border transfer prioritizes the interests of effective law enforcement and economic benefits to Indians.

There are three prominent arguments posited in favour of imposing stringent data localisation rules: sovereignty and government functions, which refer to the need to recognise Indian data as a resource to advance national interest (economic and strategic), and, further, to enable the enforcement of Indian law and state functions. The second argument is that local industry will profit economically from the development of local infrastructure, job creation,

[41] *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353.

and contributions to the AI ecosystem. Finally, in terms of civil rights, hosting locally improves security and privacy by guaranteeing the application of Indian law to the data and users' access to local remedies.

Without a question, data localisation is a representation of the state's public power. The principle of proportionality is the "paramount clause" that must be followed when exercising public power; its requirements on the necessity, appropriateness, and balance of purpose and means are of immense directional relevance for governing data localisation according to law and setting reasonable limits for it.[42] There must be a rationale behind any manner of restriction in the name of localisation. The rationale must justify the extent of the requirement of localisation putting it at a reasonable nexus with the object sought to be achieved. The test, adopted by countries globally, is a shield protecting the civil liberties of individuals and against transgressions committed by the state authorities.

Holding privacy to be a fundamental right, the Supreme Court in *K.S. Puttaswamy Case* reiterated the four-pronged proportionality test:

- ‘A measure restricting a right must have a legitimate goal (legitimate goal stage).
- It must be a suitable means of furthering this goal (suitability or rationale connection stage).
- There must not be any less restrictive but equally effective alternative (necessity stage).

[42] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, 221.

- The measure must not have a disproportionate impact on the right holder (balancing stage).'

Furthermore, Chandrachud J. drawing on the concept of proportionality, which is also used in EU law to balance competing interests, notes that any invasion of life or personal liberty must meet the three requisites of (a) legality, i.e., there must be a law in existence; (b) legitimate aim, which he illustrates as goals such as national security, proper deployment of national resources, and revenue protection; and (c) proportionality of the legitimate aim and measure adopted.[43]

The probable purpose of such a policy designed to impose limits must be defined in the first step. It should be mentioned that such a purpose must be legal. However, before deciding on the aforementioned approach, the authorities must consider the presence of any other mechanism that would advance the aforementioned purpose. The appropriateness of such a policy is determined by its implications for basic rights as well as its need. The aforementioned ruling makes it clear that the State can only use the least restrictive measure possible in light of the facts and circumstances. Finally, because the order has important implications for the basic rights of affected parties, it should be backed by appropriate evidence and be subject to judicial scrutiny. The application of this test has been witnessed in leading cases such

[43] Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' (2017) 11 IndraStra Global <https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1#:~:text=Proportionality%3A%20There%20should%20be%20a,State%20interference%20(Kaul%20J.> accessed 2 July 2022.

as in *RBI Cryptocurrency Ban Case*[44] and *Internet Ban Case*[45] where the regulations surrounding the impugned matters were dealt with in a way to maintain proportionality without infringing on the rights of individuals.[46]

VIII. BALANCING "PROPORTIONALITY" WITH DATA LOCALISATION: TOWARDS AN AMIABLE IMPLEMENTATION

The entire idea behind nations advocating for data privacy legislation and within them for data localisation standards is based on the placebic belief that the same would cater to their needs of creating a safe haven for data. However, on a deeper analysis of the subject, it is evident that the approach being undertaken is neither enough nor balanced. The proportionality test which seems like a beacon for leading us towards a digital utopia is still underdeveloped. The brief understanding of EU and Indian jurisprudence on the concept of proportionality indicates that both the jurisdictions have their own understanding and mode of implementation of the same. But what is striking is the fact that even though the ideas are not congruent they are still largely intersecting. However, the question that arises is – "How do we ensure that the implementation of data localisation stays within the four walls of proportionality without losing its essence and effectiveness?"

---

[44] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC274.
[45] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[46] Prithviraj Senthil Nathan, 'MHA Order Dated March 29, 2020: Proportionality and Necessity Arguments' (*Mondaq*, 11 May 2020) <https://www.mondaq.com/india/constitutional-administrative-law/932272/mha-order-dated-march-29-2020-proportionality-and-necessity-arguments#:~:text=A%20measure%20restricting%20a%20right,effective%20alternative%20(necessity%20stage)> accessed 29 April 2022.

The analysis clearly shows that there exist four major grounds of consideration for introducing data localization measures:[47]

- the scope of access,
- the speed of access,
- the risk of foreign retaliation against Indian firms abroad, and
- the risk of data loss due to foreign firms exiting India amid heightened regulations.

At the same time there exist four major considerations as well for promotion of economic growth which have to be taken into consideration seriously:

- demand for goods and services,
- competitive advantages for domestic producers and competitors,
- the risk of data loss due to foreign firms exiting India amid heightened regulations, and
- the risk of foreign retaliation against Indian firms abroad.

The above facts are indicative of and can act as beacons for shaping the policy. However, the key to unfolding this conundrum lies in the existing approaches implemented by the EU and India. While the need for implementing a better data localisation regime cannot be denied, at the same time it needs to be ensured that the measures undertaken are proportional and equitable to the perks they offer.

[47] cf Burman (n 4).

The major takeaway from the doctrinal as well as practical analysis of the existing jurisprudence is that any data localisation measure should be implemented within the circumscribing limits of legitimate, necessary, suitable, and balanced needs. While the strict EU grounds could be a beacon for laying down the foundation for such measures, the Indian court developed proportionality doctrine would act as the pillar for the entire structure. While it may be too early to lay down comprehensive guidelines for amalgamating data localisation and proportionality, it is however the right time to take action for ensuring the continuation of free cross-border transfer of data to fuel the ongoing globalization and development.