THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION

Submitted in partial fulfilment of the requirement of the award of degree of

MASTER OF LAW (LL.M)

(2023-24)

ON THE TOPIC

CROSS BORDER DATA FLOW AND INDIA'S DATA POLICY

Under the Guidance and Supervision of

Mr. Hari S. Nayar

The National University of Advanced Legal Studies, Kochi

Submitted by:

Vasanth B

Register No: LM0223014

Roll No: 10566

LL.M (International Trade Law)

CERTIFICATE

This is to certify that Mr. Vasanth B, Reg No. LM0223014, has submitted his dissertation titled **"Cross Border Data Flow and India's Data Policy"** in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the dissertation submitted by him is original, bona fide and genuine.

Mr. Hari S. Nayar,
Supervising Guide
NUALS, Kochi

CERTIFICATE ON PLAGIARISM CHECK

1.	Name of Candidate	Vasanth B
2.	Title of Dissertation	Cross Border Data Flow and India's Data Policy
3.	Name of the Supervisor	Mr. Hair S. Nayar
4.	Similar Content Identified	9% (Chapter 1), 11% (Chapter 2), 5% (Chapter 3), 7% (Chapter 4), 0% (Chapter 5)
5.	Software Used	Grammarly
6.	Date of Verification	24/06/2024

Checked by: Mr. Hari S. Nayar

Name and Signature of the Candidate: Vasanth B

DECLARATION

I declare that this Dissertation titled "**Cross Border Data Flow and India's Data Policy**" is researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law, under the guidance and supervision of Mr. Hari S. Nayar, and is an original, bona fide and legitimate work and it has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

Vasanth B
Reg No: LM0223014
LL.M (International Trade Law)
NUALS, Kochi

Date: 24th June, 2024
Place: Kochi

ACKNOWLEDGEMENT

The completion of this dissertation work would not have been possible without the guidance and mentorship of Mr. Hari S. Nayar, my guide and supervisor who was a pillar of support throughout. His regular inputs and meaningful suggestions meant that my work was made much easier than it could have been. I would also like to extend my gratitude to the Vice Chancellor of NUALS, Justice S. Siri Jagan and the Director of Centre for Postgraduate Studies, Prof. Dr. Mini S. Thanks also to all the other faculty members of NUALS, family and friends for their constant encouragement during the course of the writing of this dissertation.

Vasanth B

LM0223014

TABLE OF CONTENTS

Chapter 1: Introduction

There was a time when land and gold were considered the wealth of a nation. Now, the world is rapidly moving towards digitalization, e-commerce and data is being considered as the wealth of the nation. Data especially their transfer across borders have become an integral part of digital economy and play an important role in the innovation of disruptive technologies such as the Cloud Computing, Internet of Things (IoT) and Artificial Intelligence and Blockchain technologies. Hence Cross Border Data Flow is important for the International trade and for the economy of a nation. Even though Cross Border Data Flow has its economic and social benefits to a country, countries started to impose measures to store data locally within its territory to cope up with problems like threats to national security and individual privacy. Due to the absence of any cohesive and harmonious international regime several countries have developed their own national policies or legislations. Given that international legal regimes develop at a much slower pace than technological surges, some countries have adopted regional rules and guidelines. Many countries adopt different approaches to encounter cross border data flow by partially allowing trade between nations which provides the same level of security as the host country but some countries adopt the method of localizing the data within the country's territory known as the Data Localisation. Hence the research is on the various data policies and approaches India has adopted to govern cross border data flow and its efficiency in the International Trade and whether data localization can be a measure to a country like India to govern its data.

The aforementioned problems will be attempted to be addressed by this dissertation which will critically analyse the data policies of India and how they govern the Cross Border Data Flow and the problems associated with it such as the lack of International Framework and whether Data Localization can be an alternative despite its effects on the economic development of a country. Finally, solutions that could fix the aforesaid problems will be given. These include providing the type of approach that India can use to govern the Cross Border Data Flow. The Digital Personal Data Protection Act, 2023 was supposed to be the data policy but it focuses more on the data protection and privacy rather than the Cross Border Data Flow. Therefore, focus of the dissertation will remain on the studying the impact of cross border data flow in India and whether data localization can be considered as a solution. By the end, a thorough idea on what the future should hold for the International Framework on Cross Border Data Flow will be gathered.

Objectives:

- To understand and analyse the effect of Cross Border Data Flow in International Trade and India.
- To understand and analyse the efficiency of existing data policies in India in governing the cross border data flow.
- To discuss the shortcomings of the Digital Personal Data Protection Act, 2023 in governing Cross Border Data Flow.
- To analyse the advantages and disadvantages of Data Localization and whether it can be supplemented as an alternative.
- To recognise what should be India's approach in the Cross Border Data Flow considering the economic position and status of the country.

Statement of Problem:

Restrictive Trade Policies affects International Trade and according to a recent data of India, mere 1% decrease in such flows could potentially result in a loss of $696.71 million in trade for the country. With such a potential risk of loss of economy, whether Data Localization can be an alternative considering the national security and privacy of individuals in mind. Even though data localization creates job opportunities and encourages start-ups in India, it has a higher cost of production and management, it also falters the security systems and lowers the scope for developments in digital trade.

Research Questions:

- Whether there are any economic impact of Cross Border Data Flow and its restriction to a country?
- Whether India has efficient data policies to govern the cross border data flow including the Digital Personal Data Protection Act, 2023?
- Whether Data Localization can provide an effective alternative to the restriction on cross-border data flow by encouraging start-ups in India?
- What are the other approaches that India can adopt in governing data flow to increase its economy and International Trade?

Hypothesis

- A fresh set or rules or sub-ordinate legislation is needed in India addressing the shortcomings of the Digital Personal Data Protection Act, 2023 in the governance of cross border data flow and allowing for less data localisation measures because data localisation cannot be an alternative especially for a developing country like India because of its increased cost and high maintenance.

Research Methodology

- This dissertation will scrutinise international soft laws on Cross Border Data Flow such as General Data Protection Rights (GDPR) of the EU and also examine the Digital Personal Data Protection Act, 2023 to suggest appropriate approach for India.
- The research is a purely doctrinal one but will make use of already available statistical data wherever necessary.
- The sources include international treaties, executive agreements, regulations and directives of international organisations, legislations, rules, case laws, journal articles, books and other peer-reviewed articles.

Chapterisation

- Introduction
- Cross Border Data Flow and International Trade
- Data Policy of India: An analysis on the regulation of cross border data flow
- Data Localization as an Alternative
- Findings and Conclusion

Literature Review

Rajat Kathuria & Mansi Kedia & Gangesh Sreekumar Varma & Kaushambi Bagchi's (2019) report titled *"Economic Implications of Cross-Border Data Flows",* provides the recent literatures and policies which implemented data localisation in India.[1] The report also covers the economic implications of the existing and proposed data localisation measures and also its impact on the International Trade. However, the shortcoming of this article is that it covers

[1] Rajat Kathuria & Mansi Kedia & Gangesh Sreekumar Varma & Kaushambi Bagchi, "*Economic Implications of Cross-Border Data Flows"* Indian Council for Research on International Economic Relations (ICRIER) Report 19-r-20, Indian Council for Research on International Economic Relations (ICRIER), New Delhi, India.

only the economic dimension and the legal dimensions of rules and regulations was not included.

Neha Mishra's (2019) article titled *"Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?"* offers a view on the legality of the data localisation measures taken by the government.[2] It also discusses whether these GATS measures can be justified under GATS measures Art XIV (c)(ii) which aims at protecting of privacy of individuals and cybersecurity. However, the article does not delve into creating balance between trade and security policies.

Julian Rotenberg's (2020) article titled *"Privacy before Trade: Assessing the WTO-Consistency of Privacy-Based Cross-Border Data Flow Restrictions"* attempts to provide the linkage between restrictive trade practices and WTO consistency through the necessity test and chapeau requirements.[3] However it fails to address the issue of future of the cross border data flow regulations.

David J. Kessler's, Sue Ross and Elonnai Hickok's (2014) article titled *"A Comparative analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross Border Privacy Rules"* enlighten on the various sectoral policies and law adopted by India towards privacy.[4] The article also discusses the failure of Information Technology Act in addressing the privacy rights. However, the article mainly focuses on the cross border privacy rules rather than cross border data flow.

Smriti Parsheera and Prateek Jha's (2020) working paper titled *"Cross-Border Data Access for Law Enforcement"* provides the existing domestic framework that India has for lawful data access.[5] The working paper also discusses about the existing approaches for the

[2] Neha Mishra, "*Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?"* World Trade Review (Forthcoming, 2019) (Pre-edited draft) NUS Centre for International Law Research Paper No. 19/11

[3] Julian Rotenberg, "*Privacy before Trade: Assessing the WTO-Consistency of Privacy-Based Cross-Border Data Flow Restrictions*", University of Miami International and Comparative Law Review, Vol. 28, Issue 1 (Fall 2020), pp. 91-120

[4] David J. Kessler's, Sue Ross and Elonnai Hickok, *"A Comparative analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross Border Privacy Rules"* National Law School of India Review, Vol. 26, No. 1 (2014), pp. 31-61

[5] Smriti Parsheera and Prateek Jha, *"Cross-Border Data Access for Law Enforcement",* Carnegie Endowment for International Peace (2020)

data access and India's failure in taking any concrete steps towards both the international arrangements and domestic frameworks. The working paper also proposes an approach for India for the Direct Data Access by Law enforcement. However, the working paper did not update on the Digital Personal Data Protection Act and its application on the individual rights and the lawful access of data.

Joshua P. Meltzer and Peter Lovelock, (2018) working paper titled "*Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*" provides the significance of the cross border data flow in the digital trade which provides a significant share to a country's GDP.[6] The working paper also discussed the approaches for the cross border data flow taken by Asian countries. However, the article does not discuss the domestic data policies and its implications on the governance of cross border data flow.

[6] Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, GLOBAL ECONOMY & DEVELOPMENT WORKING PAPER 113 (March 2018)

Chapter 2: Cross Border Data Flow and International Trade

Part A: What is a Cross Border Data Flow?

Before entering into the cross-border data flow, one must have basic information and knowledge about what a data is? In a lay man's terms, Data is a digital version of any information about anything. Since it is a computer generated information, most people call it as computerized data.

What is Data?

The term "data" holds several interpretations and perspectives to it and the word as such "data" is not defined exclusively anywhere in any of the international agreements or conventions. So, looking into other international soft laws such as binding international treaties, executive agreements, regulations and directives of international organisations such as European Union (EU) and other texts from Organisation for Economic Co-operation and Development (OECD) and Asia Pacific Economic Co-operation (APEC) a basic knowledge that data can be categorized into three main categories: (i) Generic data or data in general (ii) Personal data and (iii) Non-personal data can be obtained. The sub-categories include Subscriber data, Meta data (Traffic data, Location data, Access data, Transactional data), Content data, Sensitive data (Health data, Biometric data, Genetic data), etc.

The term "data" is defined in the Data Governance Act of the European Union. It defines *"data"* as *"any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*"[7]. Hence, data basically means any digital representation of a fact or information or compilation of data or information in a digital form. Priority has been given much higher to the definition of "personal data" by various states and international organisations. The personal data has been defined in the General Data Protection Regulation of the European Union. It defines *'personal data'* as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,*

[7] Article 2(1) of the EU's Data Governance Act; REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022.

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[8]. The Non-personal Data as such is defined from the definition of personal data that *"Non-personal data means data other than personal data".*[9]

If looked from the perspective of Indian laws, the term data and personal data is defined in the Digital Personal Data Protection Act, 2023. According to the Act, *"data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;*"[10] and *"personal data means any data about an individual who is identifiable by or in relation to such data;"*[11]

One thing is very clear from the definitions of the personal data from both the perspectives of international law and Indian law that the legal persons such as the company and public authorities does not come under the definition of personal data unless the information about the legal person includes information which reveals the identity of a natural person. It is very clear from the definitions, as the definitions exactly says personal data means any data about an individual and not a person because the term person includes all individuals, a Hindu undivided family, a company, a firm, associations of persons, State, etc.[12]

What is cross-border data flow?

Cross border data flow generally refers to the movement of data between countries i.e. within the territory of one country to the territory of another. Or else, Cross border data flow can be defined as *"the movement or transfer of information between servers across country borders."* The international legal framework governing cross border data flow is very fragile and fragmented across policies, regional laws and trade agreements. Hence there is no universally accepted definition of cross border data flow. The cross border data flow is not a new concept as its history can be traced back to 1960s and 1970s but importance was much given when there was an increased awareness on the protection of privacy of data of individuals

[8] Article 4(1) of GDPR of EU; REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.
[9] Article 2(4) of the EU's Data Governance Act; REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022.
[10] Section 2(h) of the Digital Data Protection Act, 2023
[11] Ibid. Section 2(t)
[12] Ibid. Section 2(s)

that travels across borders. Many countries started to develop policies around the cross border data flow and data protection and international organisation also started taking initiatives to provide with a legal framework. In the year 1980, the first attempt was made by OECD by bringing in the *"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"*. This defines 'transborder flows of personal data' as *"movements of personal data across national borders"*[13]

Early initiatives were also taken by WIPO and WTO in the context of data governance and trade but the measures taken by them were considered as failure. This is because, most of the WIPO's mission were limited to the Intellectual Property and WTO has lost influence on the legal frameworks due to increasing trade protectionism measures it followed and the criticisms around the TRIPS provisions which were limiting the access to important medicines. This was not welcomed by the developing countries especially and the re-emergence of competing bilateral and multilateral trade blocs.[14] Cross-border data flows have traditionally been addressed in trade agreements. With the increase in the trend of unilateral and bilateral trade agreements across countries, there was an increase in the trade agreements explicitly mentioning the governance of data flows and localisation methods. Some of the trade agreements includes Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the US-Mexico-Canada Agreement (USMCA). Following the traditional trade agreements, the regional co-operations such as the European Union and the ASEAN co-operation also introduced their data policies which governs cross border data flows especially the flow of personal data. The European Union adopted the General Data Protection Regulation (GDPR) in the year 2016 which replaced the 1995 Data Protection Directive and the ASEAN countries have adopted the ASEAN Framework on Personal Data Protection adopted in November 2016.

With the growth of digitalization in the modern world and its influence on every aspect of economic activities is only like to expand and accelerate in the upcoming years. Cross border data flow has given rise to new information industries such as the cloud computing industries and big data analytics who rely mostly on the flow of data are now making significant

[13] Section 1(c) of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980.
[14] James McBride & Anshu Siripurapu, "What's Next for the WTO?" Backgrounder (Council on Foreign Relations, updated 13 Dec 2021).

contributions to the GDP. Cross border data flow alone has accounted for $2.8 trillion of global GDP in 2014 and its volumes is considered to be 20 times greater in 2017 than in 2007 and is likely to be expected to be four times greater in 2022 than in 2017. According to a recent McKinsey report, cross border data flow now create more value and contribute more than the traditional flow of physical goods through International Trade.[15] In the modern world, data needs to move freely across borders, so that no matter where a person is, they have the access to global range of quality information and services. Cross border data flow not only grants economic benefits but also the social benefits to the individuals, business especially the business based on E-commerce and internet based services and the government more rapidly by allowing the digital economy to flourish. Data moving across borders is very critical for the services that sustain global commerce, improve health and safety, promote social good, and enable the technologies of the future.

Significance of Cross Border Data Flow

Unlike the conventional sources of energy which drive the world right now such as the oil and fossil fuels, data does not exhibit any scarcity characteristics. It is sharable, reusable by others for a number of times and it does not deplete after every use. Companies can transfer, gather, store, process, retrieve or transmit a huge amount of data at a very minimal cost. The very interesting characteristic of data is that, its value grows with every repeated access and use by a large number of people due to accretion and network effects i.e. the value of data increases when the volume and variety of such data increases by a greater number of users having access to the same. This cross border data flow plays a vital role in all sectors but especially in the following five areas where its impact is enormous.

The cross border data flow plays an important role in sustaining global commerce. Nearly every product a person buys now depend on the global commerce and for this global commerce, vendors need to maintain and transfer the personal data of their customers and their order details. These data and their movement are very important because most global commerce rely on the third party retailers to sell and deliver their goods and therefore must maintain and move both customer and vendor data. The other aspect is the businesses which operate and function at the international level such as the hotels and restaurant chains, car and

[15] See "Digital Globalization: The New Era of Global Flows." McKinsey Global Institute, March 2016. http://www. mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

bike manufactures, freight and logistic enterprises benefit from the cross border data flow and their analytics which allows them to reach more to the local customers, improve their customer experience and can help these business work more efficiently and can reduce cost. Business of these model have to pool, gather large amounts of data which is possible only through cross border data flow. Cross border data flow can not only improve the business enterprises but also the national economies and the living standards of people in a developing country. Cross border data flow does so by leveraging global knowledge of data to facilitate national integration into the world economy.[16] A recent 2020 OECD study also found that the emerging economic participation by way of global value chains has helped the developing country industries to increase local wages and also attract foreign investments into the local infrastructure, machines and equipment development.

Secondly Cross border data flow plays a vital role in enhancing Cybersecurity. For multinational companies, one of the main requirements is the capability to collect and comprehensively analyse data which is collected across the entire organization. Similarly, such analysis is fundamental for the cybersecurity of major global service providers, such as email service providers and messaging service providers. This is because one of the safest forms of encryption right now is considered to be the end to end encryption. This requires the multinational companies to access data directly from the customer across the globe and send to another. Often to prevent these cyberattacks, necessities require not only internal analysis but also collaboration with other stakeholders in the private and public sectors. Many researchers provide data localisation as an alternative to cross border data flow security issues but storing data solely on local servers does not enhance cybersecurity; rather it is considered as a centrally stored information and is far less secure than information that is distributed across extensive infrastructures. This centralization increases the risk of unauthorized third parties breaching these data a process known as the "honeypots," potentially causing maximum harm if there is such breach as there will be large volumes of data stored locally. Distributing data storage, as seen with global cloud computing, compartmentalizes data sets, ensuring that a breach in one location is contained and does not provide access to the entire data set. Cross-border data flows also enable certain cybersecurity features, allowing companies to reduce network latency and maintain redundancy for critical data. When suspicious activity or files

[16] See, e.g., Joshua Meltzer & Peter Lovelock, Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia, Global Economy & Development Working Paper 113 (Brookings, Mar 2018).

are detected, Trend Micro, a cybersecurity company operating in more than 50 countries, automatically searches for a match in its global database of emerging threats, often blocking the spread of new attacks.

Third, cross border data flow plays crucial role in enhancing medical care and provide greater medical services and facilities. Cross-border transfers of personal data enable hospitals across the globe and other healthcare facilities to utilize clinical support software. This software analyses electronic health records of the patient, health insurance claims, and data which sets to help caregivers to enhance the effectiveness of their medical treatments and reduce risks. Personal health data that is collected has allowed researchers to identify connections between diseases, genetic factors, and lifestyle influences on the incidence of certain diseases. The COVID-19 pandemic has highlighted the critical importance of global data sharing for monitoring the spread and impact of infectious diseases, as well as for developing and administering vaccines and treatments.[17] Analysing personal health data aids health officials in early identification of pandemic outbreaks and monitoring contagion patterns, leading to quicker and more effective interventions. Additionally, it helps officials detect, characterise, and address environmental health concerns, such as spikes in ozone levels that increase cardiac arrest risks. Such advancements would not be possible without cross-border data flows.

Fourth, cross border data flow helps in the proliferation of the artificial intelligence and blockchain technologies especially in the developing countries. With the increase in the impact of digitalisation, the world is becoming increasingly interconnected through data sharing, which is driven by the emergence of artificial intelligence (AI) and blockchain technologies. For the global economy to continue growing and innovation to flourish, data must be able to move freely across borders without any restriction. The primary function of AI systems is to analyse data to identify connections that enhance the quality and accuracy of human decision-making. These AI solutions have already proven to be a transforming key sectors of the economy and society in the upcoming years, providing substantial benefits to both individuals and businesses. By using computational analysis, AI systems can uncover patterns and draw meaningful inferences with the distant instances. Restrictions on cross-border data transfers will limit the insights and advantages that AI systems can offer since it largely depends on data

[17] For a discussion of the benefits and barriers to cross-border sharing of public health data, see Marco Liverani, Srey Teng, Minh Sat Le & Richard Coker, "Sharing public health data and information across borders: lessons from Southeast Asia." Global Health at 14 (Springer Nature, 29 Sep 2018).

for its accuracy. Blockchain, a distributed ledger technology, maintains an ever-expanding list of transactions in an efficient, secure, transparent, and permanent manner. This technology facilitates international business operations by streamlining and expediting cross-border payments.

Finally, the cross border data flow helps in various other social benefits to a country. These social benefits include effective responses to natural disasters, which impact hundreds of millions of people globally each year. If the healthcare and the military forces were able to largely rely on data to locate the respondents, they can reach and provide medical care for affected civilians. In recent years, many public and private initiatives have leveraged data analytics, including the analysis of personal information, to aid in disaster response and recovery. One clear example of the benefits of cross-border data flows is the detection of credit card fraud at the point of sale. No matter where you are in the world, your bank's computer back home can analyse your purchase and location within seconds when you swipe your credit card. Based on that analysis, the system can either approve the purchase or flag it as likely fraud and prevent it. Cross-border data flows can also enhance public health, agricultural production, and law enforcement. Technological advancements in data collection and analytics can assist smallholder farmers in developing countries in meeting rising food demand under harsher climate conditions. Data obtained from satellite imagery, on-site measurements of soil conditions, and commodities markets can be integrated by computer models to predict supply and demand patterns and crop yields. This information can guide farmers via smartphone applications in selecting seeds, planting, and harvesting.[18] Additionally, cross-border data sharing can help governments tackle tax avoidance, international crime, and terrorism.[19]

Part B: Impact of Cross Border Data Flow on International Trade

Various studies have shown that the International Trade and Cross Border Data Flow have a direct co-relation to each other and international trade is proportional to the cross border

[18] For a discussion of the potential of digital technologies to help small-hold farmers, see Kenneth Iversen, Hoi Wai, Jackie Cheng, Kristinn Helgason & Marcelo LaFleur, "Frontier technologies for smallholder farmers: addressing information asymmetries and deficiencies," Frontier Technology Issues (UN Department of Economic and Social Affairs, 17 Nov 2021).

[19] For example, the UN Convention against Transnational and Organized Crime and the protocols thereto, with 143 signatories and 190 parties, contains multiple articles for improving international cooperation in law enforcement through data sharing. See United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, opened for signature 12 Dec 2000 (entered into force on 29 Sep 2003).

data flow. i.e. the international trade has increased when there is an increase in cross border data flow. Cross border data flow has led to the creation of a new aspect of international trade knows as the digital trade. Digital trade and digital technologies have become very essential to the functioning of the global economy through a variety of activities. It is even said that the modern Silk Route will be characterised by the undersea fibre optic cables and the outer space satellite connections that links and carries the electronic information from one part to the other part of the world.[20] Cross border data flow also helps in the global delivery models which are making it possible for the small workers to participate and compete in the foreign labour markets irrespective of any barriers. From the age of services being non-tradable, services now constitute a major chunk to the global GDP through the various internet and online services. WTO predicts that the share of services in total trade will increase from 21 percent to 25 percent by 2030.[21] Cross border data flow and digital trade has not only created impact to the expansion and facilitation of trade in services but also to the other sectors of the trade. One good example can be the books, music, and movie CDs are now consumed in digital formats and are known as digital goods. Digitalization has caused a decline in the trade of these goods physically, dropping from 2.8 percent of total goods trade in 2000 to 0.8 percent in 2016, according to WTO estimates. This shift has rendered geographical distances irrelevant and significantly reduced trade costs. Estimates indicate that international trade costs decreased by 15 percent between 1996 and 2014, which could support an annual increase of 1.8 percent to 2 percent in total trade until 2030, resulting in cumulative growth of 31 percent to 34 percent over 15 years.[22] Digital trade has broadened product markets and product diversity while reducing the concentration of export baskets.[23]

Underpinning the growing importance of the digital trade in the current world are the international trade transfers across borders. There is no exaggeration or it is no overstatement that most of the trade businesses today especially the Global Value Chains (GVC) rely on the data transfers for a significant portion of their operations. Naturally, this is the case not only for the GVCs but also for the companies which are engaged in the ICT and professional services sectors, but it can be stated that it is not only these sectors of trade that relies on data transfers, it is equally true for all sectors of trade, as more and more the economy moves towards the

[20] Chander, Anupam. "Trade 2.0." Yale J. Int'l L. 34 (2009): 281
[21] World Trade Report – The future of world trade: how digital technologies are transforming global commerce (2018)
[22] Ibid.
[23] Ibid.

digital trade. Cross border data flow through the international trade has provided many benefits to the consumers such as providing them with a wide range of goods and services at a lower cost. This is not possible without international trade backed by the cross border data flow. This technique is not only beneficial to the consumers but also for the business who wants to expand. Data transfer has allowed many small and medium companies especially owned by women to access IT services such as the cloud computing, data analytics, etc. which are considered to be costly investments in the local digital infrastructure. But through international digital trade, companies provide these services at a much cheaper rate. This ability of SMEs to utilise these services has enabled them rapidly scale up IT capacities and compete more readily with the big companies. For many multinationals and GVCs, the cross border data flow and digital trade is very essential even for their day-to-day businesses. The efficient supply chain management completely relies not only on the smooth flow of goods, services and capital but also on the smooth flow of ideas and managerial know-how in the form of data especially from the developing countries to the developed countries which is referred to as technology or knowledge transfer. (Baldwin, 2012).

Nowadays, it is not only the multinationals or the GVCs, firms of all sizes and across all sectors use data (National Board of Trade, 2015) for their number of operations and especially with the adoption of any new business models, it is very evident that international trade transaction takes place only with the help of cross border data flow in any sort. Cross border data flow has not only enabled us to create digital trade, it has also been the reason for the emergence of the new breed of Micro Small and Medium Enterprises (MSME)s which is currently called as the 'micro-multinational', which is 'born global' (MGI, 2016) and is constantly connected with the big globe. Data transfers and digital trade helps the MSMEs in getting access to various IT services and helped them in reducing their cost of development infrastructure. This has enabled and encouraged a lot of people to start MSMEs due to their reduced cost and who can provide services just like the multinationals with the help of cross border data flow. This scaling up has enabled the MSMEs to respond and meet with the changes in rising demand.

Earlier, one of the areas where the MSMEs lacked behind which did not enable them to compete with the big firms and was a barrier to engage in international trade was their access to critical knowledge and information but that is not the case now. Thanks to the cross border data flow and data transfers which provided MSMEs with better and faster access to critical

knowledge and information and allowing them to readily compete with the larger firms and multinationals. A recent study has shown that multinationals use the cross border data flow not only in their front desk activities but also in a large number of internal or back-office tasks and even to make routine decisions. This back desk or the back-office activities includes moving human resources (HR) data to and from headquarters, sending data to R&D facilities located abroad, managing production processes and engaging in after-sale services.[24] Data flow not only acts as an essential tool for the ordinary services but also acts as a medium for the delivery of digitally enabled services across borders which specially includes 3D printing which is a means of delivering goods, it is an asset that can itself be traded; and an enabler of trade facilitation. Considering all the above facts, it can be said that data becomes the lifeblood of trade in the digital era, measures that affect its flow are likely to have trade consequences and economic loss to a great extent to a country. In this context, trade policy makers are interested in better understanding what the consequences of emerging regulations on the movement of data might mean for trade which will have a great impact.

Raising Trade concerns

As mentioned above, the importance of data flow in the international trade, measures which affect such flow of data will also affect the international trade to a considerable extent. So, the study of such measures that affect the possibility of exchanging and moving data across borders are particularly relevant in the study of International trade. These measures mostly come in the form of conditional cross-border data transfers, and/or local storage requirements which are enabled by the countries for various reasons. With the growth in the various technologies, data policies which govern these data flows were developing in a much less pace than the technology. However, the international regulatory landscape for data flows is increasing over the years and becoming a complex framework as it is becoming difficult for the governments to seek the balance between the need for international companies to move their data across national borders and concerns for the cyber or national security and data privacy of individuals. A recent study has also shown that between 2006 and 2017, the number of data policies restricting data use domestically as well as its flow across borders has been significantly increased.

[24] See Section 4 for a more in depth discussion.

One important measure which affects the flow of data across borders is the data localisation. Data localisation is one of the most contentious and challenging policy issues in digital trade today.[25] Chander and Le define data localisation to include any measure 'that specifically encumber(s) the transfer of data across national borders. By implementing these data localisation measures which results in impeding cross border data flow and thus finally affect and disrupt various activities in the global supply chain and supply chain management. As discussed earlier, a variety of business which offers services and goods manufacturing process completely depend on the digital elements of cloud computing, Big Data processing, and artificial intelligence for most of their work.[26] By creating barriers in these data flows, data localisation measures also creates barriers in international trade thus providing the consumers with a limited variety of goods and services. For example, a data localisation law forcing local data storage or processing will increase the compliance costs as well as the infrastructure development for foreign service providers and reduces market access, particularly for small and medium enterprises ('SMEs')[27] which heavily depend on the third party service providers. Even in the absence of these particular data localisation measure which imposes strict restricts movement of data, certain other regulatory requirements (such as compliance with stringent technical standards) make cross-border data transfers impracticable.

When countries were imposing these data localisation measures, question arose among certain researchers whether these localisation measures are subject to rules under the international trade agreements especially the General Agreement on Trade in Services (GATS)[28] as it is very evident that these measures affect the cross border data flow and thus they affect variety of international trade activities such as production, distribution, marketing, sale of delivery of various internet-enabled services.[29] Applying GATS to the data localisation measures raised various questions among the researchers such as sectors affected by the measure, relevant commitments in that sector, nature and extent of violations including obligations on non-discrimination, market access, and domestic regulations and whether these

[25] See, eg, Antonio Garcia Martinez, 'The End of Data Without Borders' (1 February 2018) The Wired (online); Konstantinos Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) Journal of Cyber Policy 355.
[26] James Manyika et al, 'Digital Globalization: The New Era of Global Flows' (McKinsey Global Institute, March 2016)
[27] Matthias Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (ECIPE Occasional Paper 3/2014, 2014) 10.
[28] Marrakesh Agreement Establishing the World Trade Organization, opened for signature 15 April 1994, 1869 UNTS 183 (entered into force 1 January 1995), annex 1B ('General Agreement on Trade in Services') ('GATS').
[29] GATS art I: 1 read with art XXVIII(b).

data localisation measures can be justified under the GATS exceptions: the general exception (GATS art XIV) and the national security exception (GATS art XIV bis).[30]

Compatibility with GATS/WTO framework

When researchers conducted research on the application of GATS to the data localisation measures and were trying to answer questions like the sectors affected or the nature and extent of violation, the primary question that was posed before the researchers is whether GATS can be made applicable to the data localisation measures? There were two types of arguments proposed by two groups one stating that the GATS cannot be applied to the data localisation measures and other stating that it can be applied.

The first group of researchers argued that GATS cannot be applied because GATS was formulated in the year 1948 which is considered to be a pre-internet era treaty and thus the provisions in the GATS were not formulated keeping in mind the public policy challenges of the digital era particularly the challenges those are related to the cross border data flow via the internet of things. One such example that can be considered is that GATS does not contain any provision which explicitly mentions or requires the member to adopt domestic frameworks relating to the cybersecurity or digital privacy of individuals or the data flow affecting the national security unlike the rules that are mentioned in the recent Preferential Trade Agreements (PTA) such as the CPTPP and USMCA which contain explicit rules and commitments for the data flow of personal data.[31] Further arguments were made that GATS obligations on the states are outdated even including those that were related to telecommunication services which poses severe challenge in addressing data-related disputes.[32] Even though there were some experts who argued that the GATS provisions and disciplines

[30] See generally Daniel Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments' (Policy Brief, E15 Initiative, March 2016); generally Andrew Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2017) 19 Yale Journal of Law & Technology 182.

[31] For detailed discussion of the relevant provisions in these agreements, see Mark Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System' (Overview Paper, IDB and ICTSD, November 2017); José-Antonio Monteiro and Robert Teh, 'Provisions on Electronic Commerce in Regional Trade Agreements' (WTO Working Paper ERSD-2017-11, WTO, July 2017); Anupam Chander, 'The Coming North American Digital Trade Zone' on Net Politics (9 October 2018)

[32] Hosuk Lee-Makiyama, 'Cross-border Data Flows in the Post-Bali Agenda' in Simon J Evenett and Alejandro Jara eds, Building on Bali – Work Programme for the WTO (Centre for Economic Policy Research, 2013) 163, 164; But see Lee Tuthill, 'Cross-border Data Flows: What Role for Trade Rules?' in Pierre Sauvé and Martin Roy eds, Research Handbook on Trade in Services (Elgar Online, 2016) 357, 371; Daniel Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments' (Policy Brief, E15 Initiative, March 2016).

are just outdated and thus needs to be updated or reformed to address the unique challenges of the digitalized trade and economy.[33] Some experts also argued that the exceptions contained in the GATS Art XIV can be creatively interpreted to address the data localisation measures and to cover the contemporary policy challenges arising in the domestic internet and data regulation but this argument received criticisms that the policy objectives were clearly not envisaged at the time of formulation of the GATS to address these digital era issues and challenges.

The second group of experts argued that the GATS provisions do apply to the digital era challenges such as the data localisation measures and other challenges by the principle of evolutionary interpretation of the terms. These experts argued that even if considered that these data localisation measures cannot be applied to other GATS provisions, it can definitely be interpreted and brought under GATS Art XIV under General Exceptions. Thus, if a data localisation measure fails to comply with a Member's GATS obligations, GATS Art XIV especially under sub-clauses (a) and (c) can be used by a Member to justify derogation from its legal obligations. However, these general exceptions only cover a limited and exhaustive list of policy objectives and does not provide a broader perspective to the Member states. The data localisation measures are often taken by the governments to meet the grounds of cybersecurity or privacy. Thus, if these data localisation measures satisfy the conditions of the necessity test as well as the chapeau requirements under GATS Art XIV it can be fit into the one of the sub-sections of the GATS Art XIV. There are two sub-sections where the data localisation measures can be fitted into. One is GATS Art XIV (c) and other one is GATS Art XIV (a). First looking into GATS Art XIV (c), under GATS art XIV(c) a data localisation measure can be provisionally justified provided:

(a) it is implemented to secure compliance with domestic 'laws and regulations'[34] including those relating to:[35]

(i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;

[33] See, eg, Mira Burri, 'Designing Future-Oriented Multilateral Rules for Digital Trade' in Pierre Sauvé and Martin Roy eds, Research Handbook on Trade in Services (Elgar Online, 2016) 331, 349. See also Andrew Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2017) 19 Yale Journal of Law & Technology 182, 230-6.

[34] In Mexico – Taxes on Soft Drinks, the AB held that 'laws and regulations' refer to domestic laws and regulation, and not international law, unless it is incorporated into domestic law. See AB Report, Mexico — Tax Measures on Soft Drinks and Other Beverages, WT/DS308/AB/R (24 March 2006) ('Mexico – Taxes on Soft Drinks') [79].

[35] GATS art XIV(c)(i) (ii) (iii)

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

(iii) safety;[36]

(b) the above 'laws and regulations' are otherwise consistent with WTO law; and

(c) the data localisation measure is necessary to secure compliance with these laws and regulations.[37]

Thus, if these above provisions were interpreted in the evolutionary interpretation[38] of the terms contained in it, then they cover the different aspects of the cybersecurity and internet privacy challenges.[39] For an instance, the words law prevent 'deceptive and fraudulent practices' in GATS art XIV(c)(i) and 'safety' in GATS art XIV (c) (iii) can be interpreted and could refer to the domestic laws whose objectives are to protect consumers from cyber-crimes or other data theft from the unauthorised hacking by third parties or malware attacks, etc. The most common tool used to tackle this challenge is the prevention of data into the other territory which is the data localisation measure and the protection of the data in the host state by imposing security standards, banning malicious software or necessitating service providers to employ cybersecurity best practices. Thus, the data localisation measure imposed on the account of cybersecurity satisfies the conditions under GATS Art XIV.

Moving on to the other reason of data localisation measure which is the individual privacy, in GATS Art XIV(c)(ii) the words 'protection of privacy of individuals' can be interpreted in the context of the internet services and online services provided by the multinationals and other sectors. These measures cover the restrictions on data transfer contained in data protection laws of the host state, or should meet with other compliance requirements on part of internet service providers such as obtaining informed consent from

[36] Emphasis added.

[37] Panel Report, Colombia — Indicative Prices and Restrictions on Ports of Entry, WT/DS/366/R (27 April 2009) ('Colombia – Ports of Entry') [7.514]; AB Report, United States — Measures Relating to Shrimp from Thailand, WT/DS343/AB/R ; WT/DS345/AB/R (1 August 2008) ('US – Shrimp (Thailand)'), [7.174].

[38] For a useful discussion on the principle of evolutionary interpretation, see Gabrielle Marceau, 'Evolutive Interpretation by the WTO Adjudicator' (2018) 21 Journal of International Economic Law 791-813.

[39] In context of evolutionary interpretation, see AB Report, United States – Import Prohibition of Certain Shrimp and Shrimp Products, WT/DS58/AB/R (6 November 1998) ('US – Shrimp') [129]; AB Report, China – Publications and Audiovisual Services [396]; Panel Report, Mexico– Measures Affecting Telecommunications Services, WT/DS204/R(1 June 2004) ('Mexico – Telecoms') [7.2].While Members tend to accept GATS exception in an online context, they also favour a narrow reading of exceptions, see Work Programme on Electronic Commerce, Progress Report to the General Council, WTO Doc S/L/74 (27 July 1999) [14].

internet users or individuals and thus preventing unauthorised use of personal data. The right to privacy has been widely recognised in the online context as a fundamental human right in other international treaties,[40] with 58% countries across the world having adopted data protection laws.[41] This was because with the digitalisation and the use of smartphones, there has been raising issues of various cyber problems such as the example of third party apps using the camera of individuals without their permission in the background led to the importance of the implementation of these policies. Therefore, considering the significance of these contemporary policy concerns around individual privacy, GATS Art XIV(c)(ii) should also be interpreted to include domestic laws addressing privacy concerns in the online context.

Other provision where the data localisation measure can fit is the GATS Art XIV(a). If interpreted the words of 'public order' certain cybersecurity laws and regulations may be designed with the objective of maintaining national security and public order. Any cyber attack on the defence information or the army camps can be considered as a threat to the public order but assessment is needed in this provision to focus on whether there is a 'genuine and sufficiently serious threat to one of the fundamental interests of the society'.[42] The Appellate body of the WTO has also addressed that the notion of 'public order' can 'vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values'[43] Thus it can be stated that 'public order' in GATS art XIV(a) could be interpreted to cover measures designed to address cyberthreats affecting WTO Members.[44]

Part C: Impact of Cross Border Data Flow on India

As discussed, digitalization is the central source to economic growth forecasts for many countries and this applies to India as well. Digitalisation is said to put the nominal GDP on track to compound by more than 10 percent annually in the next decade. Knowing the

[40] See eg, Universal Declaration of Human Rights art 12; International Covenant on Civil and Political Rights art 17; The Right to Privacy in the Digital Age, 69th session, Third Committee, Agenda Item 68 (b), UN Doc A/C.3/69/L.26/Rev.1(19 November 2014).
[41] UNCTAD, 'UNCTAD Global Cyberlaw Tracker'
[42] See GATS art XIV (a), footnote 5.
[43] Panel Report, US — Gambling [6.461]
[44] In a related context, the Tallinn 2.0 Manual explicitly states the principle of sovereignty extends to 'the physical, logical and social layers' of cyberspace. One aspect of the exercise of sovereignty is the freedom to implement domestic cyber-policies including privacy and cybersecurity laws and regulations. See Michael N Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017) 13-16.

importance of the digitalisation and the digital trade, government has introduced various campaigns to proliferate the data flow. Digital India, a government campaign which aims to ensure that government services are made available to citizens electronically and is estimated to boost India's GDP between $550 billion and $1 trillion by the year 2025. This is not a big surprise even considering the large amount because India has such a huge potential and ground to make up; if the government has implemented these data trade measures in the last decade and if India had accelerated its participation in all types of global data flows, to match leading countries, then the GDP is estimated to have been $1.2 trillion higher. Other governmental efforts which are implemented by the government on Digital India for the digital transformation includes the GI Cloud (MeghRaj), a unified cloud computing initiative to attract the foreign investors and multinationals to invest in the cloud computing services of India to store the data in India, demonetization of cash especially the larger notes of Rs.2000/- to drive cashless transactions in the nation. The benefits include the payment of taxes and non-hiding of the black money and providing jobs in the digital sector. Make in India, an initiative program to encourage companies especially the start-ups and MSMEs to manufacture their products in India; and Aadhaar, a resident unique identity number program which can be accessed by the individuals anywhere. It is not only the government that is transforming into digitalization but also the private sector which is transforming digitally especially in the e-commerce and the outsourcing service sector, mainly through the use of mobile technologies and by leveraging cloud platforms to provide with cloud computing services. India has promising conditions to take advantage of new technologies in several sectors:

(i) Outsourcing: -

Data Analytics has proven to be the backbone of the digitalized economy and the digital trade. There has been an increase in the number of companies providing data analytical services in the last few years. Analytics outsourcing in India is also witnessing a huge investment through the FDI to leveraging data analytics tools to provide customized offerings of data from India. As a result of this, the analytics services industry is growing at a CAGR of 25 percent and has created $2.3 billion in 2018. The GVCs and the multinationals who operate globally rely on data being disseminated from India and other locations to make routine decisions in their day-to-day business activities especially in the cost-efficient and cost-effective manner decisions. To facilitate this decision-making process which will eventually provide added value and services to consumers, data must flow freely across international borders.

(ii) Manufacturing: -

Recent studies have shown that there is an increasing use of information on technology and sensors in the consumer technology. With this, India's manufacturing sector is planning to implement network of censors and actuators across the city for data collection, monitoring, decision making and process optimization. The government of India has introduced an initiative called the Smart Cities Mission Program which aims to provide 100 cities across the country with people friendly and sustainable environment by implementing and changing sustainable ways of manufactures, designs, and develop products in India. This mission can only be achieved if there is a standard supply chain management of data and data logistics process across the cities which can be only provided by the Internet of Things and data flow transfers. These evolutions are leading to the creation of new services in the market, known as remote factory management, which would scale up transfer of data across borders.

(iii) Financial services: -

One of the landmarks in the history of financial services of India can be said to be the demonetization program. It has helped the financial system of India in many ways. It helped to eliminate the high-value currency from the market and made evaders from the tax liabilities suffer. As an alternative, it also boosted the digital payments through the UPI which accounts each and every penny of the individual. A study shows that in the first quarter of 2017, smartphone and internet users drove mobile wallet transactions known as the UPI payments in India, which amounted to $3.6 billion—a 60 percent increase from the previous quarter. The Domestic digital payments companies benefited a lot from this initiative of the government to go cashless nation and a fintech ecosystem. This is made possible only because data is allowed to move freely without any restriction.

(iv) Health care: -

Health care industries in India has also grown considerably by the presence of world-class hospitals and skilled medical professionals who strengthened India's position as a preferred destination for medical tourism. Many people across countries have come to India to do operations because of the advanced technologies in the medical sector in India. As of 2017, the medical tourism market size was worth $3 billion, and expected to double to $6 billion in 2018.

India's regulations on the cross border data flow was previously dealt under the Information Technology Rules, 2011 which limits the transfer of 'sensitive personal data' in two restrictive ways. One is when the data is necessary and when the individual approves such transfer. Now the cross border data flow is primarily dealt by the Digital Personal Data Protection Act, 2023. This rule has further imposed data trade restrictive measures and supports data localisation measures especially in the digital payments data. Empirical evidence shows that data localization and other barriers to data flows impose significant costs, reducing India's GDP by 0.1-0.7 percent.

Part D: International policies governing Cross Border Data Flow

When it comes to international policies, there is no any specific or particular framework which governs the cross border data flow across countries. When the digitalisation of the economy started in various sectors, so does the concerns about the privacy of the individuals and cybersecurity. Hence a wide range of international instruments were proposed and adopted by various international organisations and countries in safeguarding privacy across national borders. Hence it is said that these international instruments on data protection basically govern the cross border data flow in a country. The issue and challenge with these instruments are that various countries have adopted their own approach making it difficult to come to a unilateral ground for an international framework and other challenge is to achieve privacy protection without any unnecessary restrictions on the cross border data flow. In this heading, the various international instruments proposed by various international organisations are discussed.

Organisation for Economic Co-operation and Development (OECD)

When the concerns about privacy of individuals started to emerge, countries responded in various ways. One of the first attempts by OECD to tackle this challenge, OECD came up with the 1980 OECD guidelines known as the ***"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"***. It was adopted on 23 September 1980 with the main objective of providing guidance on the collection and maintenance of the personal information especially the one that crosses the borders. The 1980 guidelines allowed the countries to restrict cross border data flow knowing that the lack of data protection in another country will affect the privacy of individual in another country. Hence importance was given more to privacy protection. Along with these guidelines, the OECD also published the 1985

Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. But later the OECD came to know the economic and social impact of such restriction on cross border data flow. Hence the 2013 update to the OECD guidelines specially calls upon the member states to "support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines."

OECD in the year 2022 published a report on ***"Cross-border Data Flows: Taking Stock of Key Policies and Initiatives".*** This report was published on 12 October, 2022. The word that is commonly used in this report is 'trust' because it is the only way of finding balance between data flow and privacy. It is very evident that people will not be engaging with companies who are perceived as non-trustable. So, companies have to co-operate with the global trust to attain the benefits of the digital trade and marketplace. This trust also plays a role in how people interact with government, enabling trust-based cross-border regulatory cooperation. The report identifies three measures to make a progression in the issue between cross border data flow and privacy with all three measures having a common aim of increasing co-operation among governments for reliable cross border data sharing. The measures are:

(i) Unilateral policies and regulations (Section 2);
(ii) Intergovernmental process (Section 3) and
(iii) Technological and Organizational measures (Section 4)

In *Unilateral policies and regulations*, the elements that are common in privacy policies of various countries were discussed. They have two things in common; one is the desire to allow cross border data flow with protection and other different policies and mechanisms in achieving this goal. These various instruments can be divided into two parts;

(i) The first is *"open safeguards"* where the assigning party or entity is given with the responsibility of protection of the public interest objectives and there are no specific ways mentioned in ensuring the same.

(ii) The second is *"pre-authorised safeguards"* where there is a greater involvement by public officer or body supervising the data transfer for reliability. Examples include unilateral whitelisting of a recipient country by the public sector, the obligation to incorporate in contracts specific clauses pre-approved by the public sector, or national certification systems whose functioning is monitored directly or indirectly by a public body. Regarding the specific clauses

in contracts, public authorities in co-operation with the privacy enforcement authorities came up with standard clauses which are considered sufficient for lawful transfer of data. Several countries have already adopted this type of clauses in their contracts between countries, including: European countries with 'standard contractual clauses' (SCCs), New Zealand, the United Kingdom, Argentina, and the nations of South East Asia (ASEAN).

In *Intergovernmental processes* the OECD has discussed about various advancement in co-operations but importance was given to the G7 and G20 deliberations. In 2019, the Japan Prime Minister declared the launch of process called 'Data Free Flow with Trust' which leads to increased co-operation among countries to provide equal data protection and allow the free flow of data. Later in 2020, G20 leaders meet in Riyadh and confirmed the agreement to 'further facilitate the free flow of data which would strengthen consumer and business confidence'. Later in 2021, the G7 Digital and Technology Ministers recognised the importance of data in the digital economy and continued to address the issue of privacy and data protection while allowing free flow of data.[45] In the year 2022, the G7 Digital and Technology Ministers declared an action plan for the DFFT to promote the cross border data flow on the basis of 'trust'. In the international organizational efforts, the OECD mentioned itself as an example where it fought for the cross border data flow and also address the issues of privacy and data protection. The OECD has always advocated the need to proceed to identify common standards on data governance in order to find the balance between data flow and privacy by reinforcing the concept of 'trust' that is found as the unitary basis of this complex subject. In this context, the OECD has issued a series of recommendations to achieve the goal of common groundwork in regulating frameworks. Among them, the important ones are:

- OECD Council Recommendation on Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013;
- OECD Recommendation on Cross-Border Cooperation in the Enforcement of Privacy Laws of 2007;
- OECD Recommendation on Improving Data Access and Sharing of 2021;
- OECD Recommendations on Digital Security, including: OECD Recommendation on Managing Digital Security Risks to Economic and Social Prosperity 2015;

[45] In 2021 the Global Privacy Assembly, a forum of over 100 data protection authorities, adopted a resolution advocating for a set of principles to be applied for government access to personal data held by the private sector for national security and public safety purposes (Global Privacy Assembly, 2021[58]).

- OECD Recommendation on Digital Security of Critical Assets 2019; and OECD Recommendation on Encryption Policy Guidelines 1997.

In addition to the above recommendations, the OECD has also produced a number of analytical reports and constantly facilitates guidelines and support on important policy issues, including with a specific focus on the policy agenda of cross-border data flows. The OECD has funded a study to outline shared principles regarding government access to personal data held by the private sector. This initiative is a crucial step in identifying commonalities in this area, where they exist, and complements other collaborative efforts to foster trust in data flows.

United Nations

Along with the OECD, the UN has also contributed to the discussions and process of implementing cross border data flow with trust. The United Nations Conference on Trade and Development (UNCTAD)'s **Digital Economy Report of 2021** addressed the issue of ***"Cross-border data flows and development: For whom the data flow".*** The report stated that there is no international balance in addressing the issue of regulating cross border data flow as the position is likely to be influenced by the major economic power countries and other digital global corporations who like to expand their global data eco-system. In spite of this, the report said that there is some convergence while dealing the main data streams. Even though, the report does not provide any solution, it paved the way for a more holistic and co-ordinated global approach in finding new and innovative ways to govern data globally (UNCTAD, 2021). In order to implement this approach and make into an action plan, in 2022 the UN Committee of Experts on Big Data and Data Science for Official Statistics launched a UN PET Lab which involved the US Census Bureau, Statistics Netherlands, the Italian National Institute of Statistics, and the UK's Office for National Statistics with the aim of providing a pilot programme that can share international data securely through PETs. The UN PET Lab has brought statistical bodies to help with the technology providers that will offer PET technologies to test solutions to transfer data across borders compliantly.[46]

World Trade Organisation

Even though WTO has not contributed much in this area in the earlier times, discussions started during the year 2017 when the WTO has focused its attention on the trade related aspects

[46] UN Stats (2022), UN launches first of its kind 'privacy lab' to unlock benefits of international data sharing

of e-commerce and e-trade. It established "Joint Statement Initiative on E-Commerce"[47] WTO released a statement in December 2021, where it recognised the importance of the cross border data flow in the high standard supply chains and commercial outcome of it.[48] To contribute to this, the WTO released a joint ***Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in the WTO Negotiations on E-Commerce*** in January 2021 which encouraged the WTO member states to negotiate and come to framework which facilitates free flow of data and secure movement across borders.[49]

World Bank

The World Bank has also contributed to the discussions on the cross border data flow by establishing the ***"World Development Report 2021: Data for Better Lives"*** which answers the questions that were posed before the World Bank about the governance of data in a safe, ethical and secure way by not restricting the flow of data. With special reference to cross border data flow, it stated and argued that data will have a central and expanding role in the upcoming business models and it will reshape the competition, international trade and taxation in real economy. If the cross border data flow is not governed properly, it will pose a risk to the low and middle-income countries. Hence the report suggested for an internationally coordinated approach on antitrust enforcement, regulation of data providing platforms, data standards, data clauses in the trade agreements and tax policies in a nation to ensure efficient, equitable policies for the data economy that respond to countries' needs and interests.

When international organisations were struggling to find a common ground for the framework on data governance, several countries and regional co-operations adopted different approaches for regulating data especially the personal data protection making the situation of governing cross border data flow worse. The regional approaches taken by these countries were enacted according to their own whims and fancies and hence they tend to vary to a very large extent in governing data. The other issue with regional frameworks is that some of them are not open for every country to adopt making them restrictive in nature. Some of the notable regional frameworks includes:

[47] WTO (2017), "JOINT STATEMENT ON ELECTRONIC COMMERCE", Ministerial Conference, World Trade Organization,

[48] WTO (2021), "Statement by Ministers of Australia, Japan and Singapore", Joint Statement Initiative on E-commerce,

[49] ICC (2021), Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce

Convention 108 of the Council of Europe

The very first major framework on the protection of personal data of individuals adopted by European countries majorly is the ***1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,*** commonly referred to as ***Convention 108 of the Council of Europe.*** This treaty was primarily dealing with protecting the right to privacy of individuals with respect to personal data that are automatically processed. This convention was put forth for signatory and till date there are fifty-three states, mostly European countries signatory to the convention where the states have committed to establish data protection under their own domestic law, sanctions and remedies for violations of the Convention's provisions. This convention was modernized in the year 2018 known as the "C108+". The new protocol as well as the previous one provides that countries should not restrict the flow of personal data between states signatory to the convention unless if there is any situation which is classified under exceptions such as transfer could lead to the circumvention of the provisions of the Convention and transfer to a non-signatory country can only be done when the latter provides the same level of protection in the recipient entity. However, the recitals of the EU's GDPR indicate that a third country's accession to Convention 108 and its implementation would be a significant consideration in applying the European Union's international transfer regime, especially when evaluating whether the third country provides an adequate level of protection.[50]

General Data Protection Regulation (GDPR)

When the technology was progressing with the emergence of the internet in the mid1990s, the EU recognized that they should have a framework to govern the data protection in the modern world. So, the EU passed the ***European Data Protection Directive*** in 1995 providing a minimum guaranteed protection on data privacy and security standards which each must comply with their national laws. But with the emergence of rapid development in the data and the technological sector in the 21st century, the EU thought that with the Data Protection Directive they can't handle the modern challenges and thus need a complex framework and thus began to update the 1995 Directive. Thus, the ***General Data Protection Regulation***

[50] Official Journal of the European Union (2016), 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

(GDPR)[51] emerged and entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.

The EU's General Data Protection Regulation (GDPR) provides a comprehensive approach and is also considered to be the toughest privacy and security law in the world. Article 2 of the GDPR has defined a handful amount of terms relating to the data protection such as the 'personal data', 'data processing', 'data processor', etc. Article 5 lays down the data protection principles where the data processing must be lawful, fairness and transparent, there should be purpose limitation and data minimisation, etc. Article 6 enlists the circumstances in which it is legal to process the personal data such as the necessity, to perform a task in public interest, etc.

The GDPR adopts a horizontal approach on the governance on cross-border data flows and personal data protection where the GDPR prevents transfers of personal data to another jurisdiction that has not been deemed by the EU to have adequate privacy protection and the term adequacy privacy protection was interpreted by the European Court of Justice where it found that a finding of adequacy requires the other country to provide privacy protection that is "essentially equivalent" to that found in the EU.[52] Where the recipient country cannot provide such a protection, then the EU does not allow transfers of data to such entities in 'non-adequate territories' but if the transfer is conducted according to the binding corporate rules or the "standard contractual clauses" in the trade agreements which is approved by the Data Protection Authority, then the transfer can happen to such entities. The problem is and also the reason why it is called the toughest privacy law is because so far, only a handful of countries have received an adequacy determination from the European Union.[53] The need for an adequacy decision from the European Union in order to transfer personal data creates an economic incentive for other countries to seek such a finding.

APEC's Cross Border Privacy Rules

Another regional co-operation which holds hand in the privacy data protection is the Asian Pacific Economic Co-operation (APEC). The APEC has formulated the Cross Border

[51] Regulation (EU) 2016/679.
[52] Schrems v. Data Protection Commissioner 2015, para 94.
[53] Countries with an adequacy finding as of February 2018: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US under the Privacy Shield.

Privacy Rules (CBPR) in the year 2011 to govern and facilitate the transfer of privacy data among the members of the APEC countries. The Cross Border Privacy Rules was introduced as a voluntary one where it is not binding on all the APEC countries and even when an economy adheres to Cross Border Privacy Rules, it can choose whether to seek certification under the system. Currently it has 9 member states including big countries like USA, Japan, etc. Unlike the right-based approach of the EU in GDPR, the Cross Border Privacy Rules are principles based where it allows governments with greater flexibility in designing their domestic legislations to provide the data protection that comports with the APEC privacy guidelines and need not have to be adequate which is in the case of GDPR. Unlike the GDPR, where the responsibility and accountability are on the government who shares the data, here the business entities who collects the data and transfers either domestically or to any third countries are made responsible to protect the data consistent with the APEC privacy principles.

In addition to it, the CBPRs also require business entities to develop their own privacy policies based on the APEC privacy principles and which meet the CBPR program requirements.[54] The CBPR has also established the APEC Accountability Agents whose role is to assess these business privacy policies and practices and ensure consistency with the APEC CBPR requirements.[55] There is only one pre-condition to participate in the APEC Cross-Border Privacy Rules which is that the government which is participating should have at least one privacy or data-protection enforcement authority participating in the APEC Cross-Border Privacy Enforcement Arrangement which is the framework formulated for regional cooperation in enforcement of privacy and data-protection laws among APEC member economies.[56]

Preferential (PTA) and Regional Trade Agreements (RTA)

Since the WTO was working on a very slow pace in the context of governing the cross border data flow and the economic advantages of data flow were raising, many governments started parallel to address the issues of cross border data flow and trust in the context of both personal and non-personal data in their preferential trade and digital economy agreements. Since the year 2008, there has been a significant increase in this addressing of cross border data flow in trade agreements, till the year 2020 29 agreements involving 72 economies have

[54] CBPRs 2015.
[55] APEC CBPRs: Policies, Rules and Guidelines, 10.
[56] APEC CBPRs 2017.

introduced some form of data flow provisions.[57] The depth and governance of these provisions differ from agreement to agreement. Around half of these agreements which were formulated in earlier times didn't give much importance and hence they had non-binding guidance on data flows. Examples of such agreements are the Korea-Peru Free Trade Agreement (FTA) and Central America-Mexico FTA. Whereas the trade agreements that were formulated in the last 5 years, contained binding provisions on data flows which includes all types of data. Notable trade agreements in this area are the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[58], New Zealand Ministry of Foreign Affairs and Trade[59], the United States, Mexico, and Canada Agreement (USMCA) and the EU-UK Trade and Cooperation Agreement. Regarding this, CPTPP states that

"Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means". However, "each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person"[60]

Whether containing binding provisions or not, all these agreements included exceptions where it allows parties to restrict data flow "legitimate public policy objectives" and the other important characteristic is that all these trade agreements includes provisions on the need for domestic privacy legislation and references were also given to the inter-governmental processes. Due to these advantages, governments were increasingly using the trade agreements to find the balance between the data flow which is essential for the trade in digital era and also the cross border data flow that is accompanied by safeguards for personal data protection, including via reference to inter-governmental arrangements. With advancements in the technology in digital trade, countries have also started to include them in the clauses. Recently, the EU-UK Trade and Cooperation Agreement (TCA) has also introduced a clause stating that *"measures on the protection of personal data and privacy, including with respect to cross-border data transfers"* will also include *"instruments enabling transfers under conditions of general application for the protection of the data transferred".* Knowing the economic impact of the free data flow and restricting the same by data localisation measures, these agreements

[57] Casalini, F., J. López-González and T. Nemoto (2021), Mapping commonalities in regulatory approaches to cross-border data transfers.
[58] Parties to CPTPP are: Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Viet Nam.
[59] New Zealand Ministry of Foreign Affairs and Trade (n.d.), Comprehensive and Progressive Agreement for Trans-Pacific Partnership text and resources,
[60] Article 14.10 of CPTPP

have increasingly included provisions to prohibit the same. CPTPP (see Article 14.13) and USMCA (see Article 19.12) have provisions which state that computing facilities be located domestically as a condition for conducting business is prohibited generally.[61] Additionally the USMCA has a provision which states

"No Party shall prohibit or restrict the cross-border transfer of information and applies similar provisions as above for exceptions."[62]

Even with the efforts of international organisation, data governance is still lacking behind in meeting new frontier technologies. Hence, countries have also started negotiating broader digital economy agreements (DEAs) which governs a wide range of issues, starting from artificial intelligence, blockchain technologies to e-payments. These new types of trade arrangements often include binding provisions on both maintaining personal data protection frameworks which shows importance is given to privacy and at the same time allow cross border data flows, subject to certain exceptions. For example, the United Kingdom and Singapore have signed a Digital Economy Agreement (UKSDEA) in 2022.

U.S.-EU Privacy Shield

The USA and European Union being the two drivers of the world economy, found difficulty in transatlantic exchanges of personal data for commercial purposes between them. This is because these two governments have different approaches where the US data governance is primarily based on the domestic legislations and federal laws whereas the European countries had the General Data Protection Regulation (GDPR). Hence both the governments have negotiated to formulate the U.S.-EU Privacy Shield in the year 2016 and this has been deemed to have satisfied the adequacy test by the European Commission. This allows for the free flow of data even the personal data between the European Union countries and business entities in United States. The privacy approach taken under Privacy shield is that the U.S. companies should self-certify themselves before the U.S. Department of Commerce that they will protect personal data consistent with the Privacy Framework, which also includes the Privacy Shield Principles. In addition to this, the UN businesses should also publish their privacy policies under the Privacy shield and gives the U.S. Federal Trade Commission

[61] Nemoto, T. and J. López González (2021), "DIGITAL TRADE INVENTORY RULES, STANDARDS AND PRINCIPLES OECD TRADE AND AGRICULTURE DIRECTORATE Digital Trade Inventory: Rules, Standards and Principles".
[62] Article 19.11 of USMCA

jurisdiction over such businesses if they breach their own policy. The U.S. is also required under the shield to provide various redress means for the people whose personal data is compromised in the course of economic operation, which includes a direct complaint to the business or a complaint to the Department of Commerce. Privacy shield also includes a provision which establishes an ombudsperson to address complaints about government agency requests for information transferred to the US from the EU or Switzerland on the basis of national security. The U.S.-EU Privacy Shield is a perfect example where the difference in approaches between the EU approach to privacy and the U.S. accountability-approach might find a balance. In this regard, Privacy Shield provides exception to a country like the U.S. not having to adopt a difficult privacy regime like the EU's GDPR. Instead, Privacy Shield allows a subset of businesses in a U.S. to agree to a particular privacy regime particularly the domestic legislations in order to be deemed equivalent by the EU. This enables the free flow of personal data between the EU and the business participating in Privacy Shield.

The U.S. Approach

While the U.S. Constitution does not specifically protect privacy, there is a long-standing tradition in the U.S. of valuing privacy protection and the development of privacy principles by the courts. For example, in the 19th century, Samuel Warren and Louis Brandeis, concerned about media intrusion into personal lives, wrote about a "right to be left alone" (Warren and Brandeis, 1890). The U.S. Code of Fair Information Practices, based on Fair Information Practices Principles (FIPPS) developed in the 1970s, laid the foundation for various U.S. laws governing the collection and use of personal information by the federal government and influenced the OECD Privacy Principles of 1980.

The current U.S. privacy framework is built on a broad set of privacy laws that apply to the federal government, such as the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and the Right to Financial Privacy Act of 1978. For the private sector, personal data protection is governed by sector-specific legislation, including the Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act. Privacy protection in the U.S. emphasizes notice and consent, with the Federal Trade Commission (FTC) responsible for enforcing companies' compliance with their privacy policies. Additionally, individual U.S. states have their own data protection laws. Unlike other approaches that impose specific cross-border data restrictions,

the U.S. approach relies on the application of domestic laws to hold companies accountable for breaches of their privacy notices. This system makes individual companies responsible for ensuring the privacy of personal data both within the United States and internationally.

Hence these are the various international and regional policies and approaches taken by regional organisations and countries in the governance of cross border data flow. From a study of these guidelines and approaches, it is very evident that there is no uniformity among these approaches in governing the data transfer as each country has their own interest surrounding the allowance and restriction of data which makes international co-operation in the area of cross border data flow very difficult.

Chapter 3: Data Policy of India: An analysis on the regulation of cross border data flow

Though India has taken various steps in digitalizing its economy and other governmental activities through various initiatives such as the Digital India, etc., the Indian Legal Frameworks which governs data has not kept pace with the growth in digitalisation. With the government adoption of the new technologies and services, debates arose in India about the balance in meeting the data protection and digital innovation that has accelerated.[63] When we speak about governing data and data protection, importance is always given to personal data not only in India but also around the world. In most of the countries, such forms of personal data protection laws set out what can be done and what cannot be done with the personal data that is collected and ensure that individuals have their own control of who they are sharing their data and most often they become the data policies of the country. In India, various laws were indirectly governing the data but with the implementation of Digital Personal Data Protection Act, 2023 it stands as the comprehensive legal framework for data protection and privacy rules. Whether it addresses cross border data flow and every aspect of data protection is still a question that needs answer.

Part A: History and Background

The data policies of India can be traced back to period before digitalisation was even in existence. The data policies in India was not formulated in the recent times as its history can be found in the 18th and 19th century when the Indian Telegraph Act, 1885 and the Public Records Act, 1993 were enacted. The Indian Telegraph Act, 1885 governed all the wired and wireless communication and data during that period and the Public Records Act, 1993 contained a provision which imposes data localisation measure at that time where it states that "*No person shall take or cause to be taken out of India any public records without the prior approval of the Central Government: Provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose."*[64] After the same, importance was given to data protection when the digitalisation started to emerge in various

[63] Arvind Gupta and Philip E. Auerswald, "The Ups and Downs of India's Digital Transformation," Harvard Business Review, May 2019, https://hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation.
[64] Section 4 of the Public Records Act, 1993 ACT NO. 69 OF 1993 [21st December, 1993.]

economic activities and since cyber related activities and crimes were governed by Information Technology Act, 2000, amendments were made to the act and its rules to govern the data protection and privacy.

Information Technology Act, 2000

When the digitalisation was growing to its peak and when awareness started among people about their data privacy, the Information Technology Act, 2000 ("IT Act") was the only legislation which tried to attempt to address the issue of data protection. The idea of data protection was first mooted in Indian Parliament in 2008, when they brought in an amendment called the ***Information Technology (Amendment) Act, 2008***. The amendment introduced a new Section 43 A which states *"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."* Thus, the new section imposes obligations on the companies whoever collects personal data to protect such all sensitive personal data and information that they posses or deal or handle by way of a computer resource. The amendment also imposed a penalty for not complying with the same but the section was not considered adequate because it even failed to describe what a sensitive personal data is. Hence, the amendment was followed by the ***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.*** This rule served as a basic framework for the protection of privacy and personal data.[65] Even though these rules didn't provide a comprehensive legal framework to address complex issues like the regulation of children's data rights, cross border data transfers or establishment of any data protection agency or body, they dealt with basic challenges of collection, possessing, storage, handling, retention, transfer, and disclosure of sensitive personal data by corporations through the introduction of a consent requirement for all such activities. The law also prescribes certain "security practices and procedures" for the handling of sensitive data.[66]

[65] Indian Ministry of Communications and Information Technology, "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011," Indian Ministry of Communications and Information Technology, April 11, 2011

[66] Indian Ministry of Electronics and Information Technology, "White Paper of the Committee of Experts on a Data Protection Framework for India," Indian Ministry of Electronics and Information Technology

The Information Technology Rules 2011 in a way addressed the cross border data flow by stating that personal data can be transferred across border but under two conditions that when the transfer of data is found to be necessary for the performance of any lawful contract between the corporate body or any person and the provider of information, or when the individual who provided the data consents for such transfer across the country. Although these rules have come a decade before, insufficient administration and delays have made it hard to implement these rules in the real situations.[67] Companies who have to comply by these rules found it very hard because of the ambiguities posed by the rules and companies received only limited or no guidance in addressing these ambiguities.

National Data Sharing and Accessibility Policy, 2012

When the concerns arose about personal data, government also started thinking of policies governing government data. In 2012, India enacted a "National Data Sharing and Accessibility Policy", which primarily governs the government data i.e. the data that is owned by government agencies and/or collected using public funds. The policy also imposes a data localisation measure just like the Public Records Act, 1993 that these government data must be stored in local data centres. This policy not only acts as a governing framework but also acts as a public portal which makes disparate government data assets available for public to access. However, the policy only includes non-personal and non-sensitive government data that is generated using public funds across all levels and departments of the government and its agencies. The policy also covers a wide range of data including all digital, analogue, machine- and human-readable formats, and suitable payment structures which has been created by the government to incentivize data sharing. As mentioned, the government took a technological approach in making the data available to public by developing the ***Open Government Data Platform***. After the launch of this program in 2012, several other data programs such as the India Urban Data Exchange of the Ministry of Housing and Urban Affairs, Open Budgets India created by the Centre for Budget and Governance Accountability, National Data and Analytics Platform by NITI Aayog, etc. have been launched.[68] This received a positive approach as these

[67] Sreenidhi Srinivasan and Namrata Mukherjee, "Building an Effective Data Protection Regime," Vidhi Centre for Legal Policy, 2017, https://www.scribd.com/document/338204284/ Building-an-effective-data-protection-regime-in-India.

[68] India Urban Data Exchange, "Unleashing the Power of Data for Public Good," India Urban Data Exchange, https://iudx.org.in; Open Budgets India, "Making India's Budgets Open, Usable, and Easy to Comprehend," Open Budgets India, https://openbudgetsindia.org; NITI Aayog, "National Data and Analytics Platform: Vision Document," NITI Aayog, January 2020

data platforms offers more information and data to all the users which made the public to benefit out of the governmental programs that were enacted by the government and they also support the functionalities for social media, data visualization, and data suggestion and help in strengthening their utility.

Hence to improve the data access, the Indian government has introduced a revised draft of the India Data Accessibility and Use Policy and a draft of the National Data Governance Framework Policy.[69] The draft of the National Data Governance Framework Policy mainly focuses on the sharing of non-personal data which is collected by the government or its agencies from Indian citizens and residents through the India Datasets Program. This policy establishes a new framework for governing citizens' data, which includes the formation of the Indian Data Management Office. This office will create an extensive repository of Indian data sets and set standards for their storage and collection.

Impact of Puttaswamy case

A Constitutional Bench of nine judges of the Supreme Court of India in the year 2017 in the case of ***Justice K.S.Puttaswamy (Retd.) v. Union of India***[70] upheld that right to privacy is a fundamental right which can be entrenched under Right to Life and Personal Liberty provided under Article 21 of the Constitution. This judgment laid the foundation for the single statute legislation which governs the data protection in India i.e. The Digital Personal Data Protection Act 2023 by the formulation of Sri Balakrishna Committee. In this case, the SC compared 'privacy' as a basic element of the right to life and liberty and so the 'right to privacy' is also considered as a fundamental right. When dealing with the case, the Supreme Court not only dealt with the rights of citizens against the state and the obligations of state, the judgment also laid down that protection must be provided to individuals in the private spheres including the online data. The Supreme Court linked right to privacy to individual dignity and stated that states always have a positive burden in maintaining and preserving this dignity. Hence, the Puttaswamy Judgement was considered not only as a basis for state action and individual rights but it also provided a basis for the obligation of the state in governing the private contracts who collects and shares the private data in the interest of individual privacy.

[69] Indian Ministry of Electronics and Information Technology, "India Data Accessibility and Use Policy (Draft)," Indian Ministry of Electronics and Information Technology, February 2022
[70] AIR 2018 SC (SUPP) 1841

Sri Balakrishna Committee Report

After the impact of the Puttaswamy Judgment, public awareness arose to its peak about the right to privacy and the government were in a position to enact something for the same. So, in the year 2017, the Ministry of Electronics and Information Technology on behalf of Government of India, appointed a ten member committee with Justice B.R. Krishna who is a retired Supreme Court judge as the chairperson. This committee was constituted to work on the introduction of the data protection framework in India and provide a report. After the continuous efforts and deliberate work of the committee for a year, the committee finally submitted its draft report titled "***A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"*** on July 27, 2018. The committee report is the first of its kind to define the term 'personal data'. It stated *'personal data' is any kind of data that allows identification of an individual, whether directly or indirectly*. The committee also made a clear distinction between sensitive personal data and critical personal data and in its report made separate provisions for collection and processing different kinds of data. It stated that sensitive personal data relates to more intimate matters of the individual such as caste, religion and sexual orientation of such individual whereas critical personal data may include previous health records, blood type, etc. of the individual.

The report also suggested that the critical personal data should be processed in the centres and stored that are located within the country only. The reports also recommended that there should be a fiduciary relationship between the service provider or the business entities who collects data and the individual whose data is collected. This fiduciary relationship puts an obligation on the service provider to deal with the personal data of the individuals in a fair, transparent and legitimate manner and also to give the individual notice of data collection at various points and also information about what type of data is collected and the data shall be collected only after the consent of the individual. This consent may at any time be withdrawn by the individual. The report also introduced the concept of 'purpose limitation principle'. This principal state that personal data collected should be limited only to that purpose in using and the purpose mentioned should also be very specific. The principle also includes lawful purpose as well. The report gave a special mention to the data of the children. It stated that stricter provisions are needed for the protection of their data.

The report also recommended that all the service providers and organisations whoever collects data should definitely appoint data protection officers. These officers will be the point of contact for the users whose data is collected and if they have any grievance in data collection by the concerned organisation, they may contact these data protection officers. Unlike the Information Technology Amendment Act, 2008, this committee recommended a high penalty for non-compliance by the organisations where penalties range from percentage of 2 to 4 of the company's turnover and worldwide turnover in case of international business or fines for a amount between Rs. 5 crore and Rs. 15 crores, whichever is higher. One of the important highlights of the report is that it does not make companies who only process the data liable, the obligations includes for all companies who use, store, disclose or collect the data anywhere in India and thus providing a broader scope for protection of data.

The report also recommended for the setting up of data protection authority which would be an independent regulatory body under the government which will be responsible for the overall governance over the company's action and for the enforcement and implementation of the data privacy law. The report also suggested that this body is also imposed with an additional duty to conduct legal and sociological research to provide with better clarity on the implementation of law. The committee also recommended setting up of an Appellate body and decisions of the Data Regulatory body can be challenged in the Appellate body. The committee also recommended that certain rights must be vested in the hands of the individual such as the right to access their data, to correct it, withdraw their consent, right to object to the data processing, right to be forgotten, etc.

The Balakrishna committee report made a whole lot of recommendations for non-personal data as well. The committee defined nonpersonal data as "*data that never related to an individual (such as weather conditions or data generated from public infrastructure, to cite a few examples) and information that was once personal data and subsequently was anonymized in such a way that it cannot be used to identify an individual (such as anonymized healthcare records of patients).*" Just like the Data Protection Authority, the committee also recommended for the formulation of a separate Non-personal Data Authority. The committee recommended that this authority will be working closely with the Data Protection Authority but primarily focusing on the governance of the non-personal data. The committee also suggested a framework for the regulation of non-personal data which is distinct from the personal data in its report. One of the report's key recommendations was to create high-value

data sets. All data businesses will be mandated to submit metadata for all nonpersonal data they control. This metadata will be stored in a centralized directory and managed by the Non-personal Data Authority.

Personal Data Protection Bill, 2019

After the recommendations of the Sri Balakrishna committee, the Draft Personal Data Protection Bill was created in the year 2018 and was sent to various industry and stakeholders for their feedback and was made available to public. After hearing the feedbacks and suggestions, the draft bill was amended and in December 2019, the Ministry of Electronics and Information Technology tabled the ***Personal Data Protection Bill 2019 (PDPB)*** in the Parliament. This bill is considered to be the India's first overhaul legislative framework for regulation of data sharing in private contracts. This bill followed most of the recommendations of the committee and has prescribed compliance requirements for all forms of personal data, vested a lot of rights to the individuals regarding data privacy, introduced a central data protection regulator who will be governing the actions of private contractors, also imposed restrictions on the cross border transfer of sensitive personal data and as well as imposed huge financial penalties in case of non-compliance. The bill was considered to have a challenge in its implementation and was sent to Joint Parliament Committee for review. Due to the global pandemic issue, the Joint Parliament Committee took nearly 2 years to work on the bill. The said bill is considered to be focused mainly on personal data as the bill mentioned to regulate non-personal data in only two provisions.[71]

Two clauses include the clauses on the breaches involving non-personal data and the clauses on the obligation of data fiduciaries to provide the central government with non-personal data for the "targeted delivery of services" or "evidence-based policy making".[72] Since there is no proper comprehensive framework for non-personal data, in the meantime the Ministry of Electronics and Information Technology released a report called as the ***Non-Personal Data Governance Framework*** in July 2020. Since the non-personal data holds so much value to it, the intention behind creating this framework is to possibly gain the economic, social and especially the commercial value of non-personal data for corporates, start-ups and

[71] Dvara Research, "Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019," Dvara Research.
[72] DP Bill Section 92(2) and 94(2)(e); and Prahalad Sriram, "Reconciling Localization Mandate of the Personal Data Protection Bill, 2019 With International Trade Obligations," Narsee Monjee Institute of Management Studies (NMIMS) Law Review 2 (June 2020): 273–284

the Government. When the report was released, the committee received over 1500 responses from various stakeholders. Based on the responses, the same committee released the revised Non-Personal Data Framework in January 2021. This revised report limited the scope and purpose of utilising the non-personal data and focused on how the proposed Personal Data Protection Bill and this Non-Personal Data Framework can go in hand together.

Data Protection Bill, 2021

After nearly two years of scrutinization by the Joint Parliament Committee, the JPC finally submitted its final report and the draft bill in November 2021. In the new proposed bill, the Personal Data Protection Bill was renamed to ***Data Protection Bill, 2021.*** The key change brought to the bill which is also the reason for the change in name is that proposed bill is said to cover not only personal data but also non-personal data. The committee reasoned this by stating that it is very hard to distinguish between the personal and non-personal data and hence non-personal data should also be included under the ambit of Data Protection Bill. The new bill also introduced various other changes such as stringent data breach reporting requirements such as the obligation on the data fiduciary to report within 72 hours about any data breach, regulation of hardware manufactures and enabling a certification mechanism for all digital and IoT devices. The committee also imposed immense powers on the Central Government such as prior consent from central government for cross border transfer of sensitive personal data and power to exempt certain agencies from the obligations under the bill to protect the public interest.

The expectation from the public was that the proposed Data Protection Bill, 2021 will be placed in the budget session held in February 2022 but the proposed bill received strong criticisms from various stakeholders such as the wide powers were vested in the Central Government, instead of focusing on the right of individuals and protection of data it focused mainly on the state's interests and other strong criticism was the data localisation measure in the proposed bill. The Digital Data Protection Bill, 2021 required all the tech companies to mandatorily store in India a copy of sensitive personal data that is collected by the company. The bill also imposed restrictions on the cross border transfer or export of any critical personal data. This received a lot of criticism even within the Joint Parliament Committee as it is difficult for the domestic and international business to comply with the same which led to its withdrawal.

The Digital Personal Data Protection Bill, 2022

After receiving very strong criticisms, the bill underwent important changes and the new bill ***The Digital Personal Data Protection Bill, 2022*** was introduced in 2022. Unlike the previous bills, this bill has brought in a lot of significant changes. Unlike the previous bills, the number of clauses in this bill was reduced to 30, it completely rejected the personal data in physical format as the digitalisation was increasing and importance was given to digital data and it does not separate or categorize personal data into any kind like the sensitive or critical personal data. The bill also clears ambiguity about the death of data principles where now they are empowered to nominate another individual to exercise their rights in case of their death or incapacity. Since the previous bills received strong criticisms for the data localisation measures, the new bill allows the data fiduciaries to transfer the personal data outside the territory under certain exemptions. Unlike the previous bills, the new bill struck down the data protection authority and appellate body and came up with the Data Protection Board of India which will be responsible for data governance and appeals from the board will be dealt by the High Courts of India. This bill also introduced a new concept called the 'Deemed Consent' from data principles. The concept states that even if data principles didn't give their consent and their data is collected or processed, it is deemed that data principles have given their consent. Even though the bill illustrates certain situations where it deemed consent can be used, some of these situations include vague terms like 'pubic interest'.

The term public interest is a very broad term and lot of arbitrary acts can be covered under the term of public interest. Many stakeholders have raised concerns about the misuse of this concept of deemed consent as it is very vague and unclear. It is suggested that government must limit its vagueness by introducing a clear subordinate legislation or rules. This bill like the previous bills imposes heavy financial penalties on non-compliance but here the range or quantum of penalty is capped in terms of money and no relation to the worldwide turnover of the company as it is very difficult to find the value and it is an unreasonable procedural burden on the part of the government. One common thing is that this bill also vests a lot of power on the Central government such as the waiving of applications of the provisions of bill in the interest of the state or to maintain any public order. Even though the new bill clears certain ambiguity in the previous bills, there are not sufficient provisions for an effective implementation of the bill. Hence this bill needs an effective subordinate rule or legislation to create a great impact on the data protection and governance in India.

Part B: The Digital Personal Data Protection Act, 2023

After nearly 4 years of struggle in the privacy law and certain amendments to the 2022 Bill, the Digital Personal Data Protection Act, 2023 got the consent of the president and was enacted on 11th August, 2023. The Digital Personal Data Protection Act, 2023 is the first comprehensive legal framework on the data protection and privacy laws in India. The Act has varying features and characteristics such as providing various privacy rights to individuals such as right to erase, alter, use of data or withdrawn the consent already given to a particular data, etc. The act gave much importance to the consent provided by the individuals as it is necessary in every step of collection and process. The act also imposes immense obligations on data fiduciaries in collecting and processing the data. The act also established the Data Protection Board of India under Section 18 of the Act and also established a class of fiduciaries who may be notified by the Central Government as Significant Data Fiduciaries under Section 10 of the Act.

Governance of Cross Border Data Flow

India's approach towards the governance of cross border data flow has been a rollercoaster with ups and downs. At present, the Digital Personal Data Protection Act, 2023 governs the cross border data flow or data transfers of India where it has established a fundamental ground on data localisation. Section 16 of the DPDP Act, 2023 governs with the cross border data flow. Section 16 states that it allows the Government of India to restrict the flow or transfer of personal data to a country or a place outside the territory of India which the Government will notify through a notification. This is called the blacklisting of countries where the data will not be transferred to the countries in the said list. This also states that there is no any default restriction on the cross border data flow. The data can freely flow to a country without any restriction if the said country is not in the list. This move by the government in likely to be less restrictive on the approach of data localisation by the government, especially when compared to the previous bills. According to the Act, it is likely that the Central Government after making an assessment in various factors which it will consider to be necessary, notify the countries or territories outside India to which Data Fiduciaries who collects data should not transfer any personal data. Whereas till now, the Central Government hasn't notified any list of countries.

Continued application of Sectoral Laws

Where Section 16(1) of the DPDP Act, 2023 has provided a baseline protection with respect to all kinds and categories of personal data irrespective of any sector or collected by any data fiduciary, Section 16(2) explicitly states that the restrictions that are already in existence by the laws of India which provides any additional requirement or higher degree of protection will also continue to apply. This provision gives autonomy to the sectoral regulators where if they think necessary, can impose any data localisation or data restriction measure depending on the nature of data or needs of industry. At present, there are several data restrictive measures imposed by several sectors which restricts cross border transfer of data in India. One good example is the restriction imposed by the Reserve Bank of India which is the India's banking regulator has imposed data restriction that critical categories of payment details such as the transaction information and customer credentials can only be stored only within the territory of India. Other sectors of India have also imposed restriction such as the telecommunication department has imposed restriction on data relating to accounting information relating to subscribers cannot be transferred outside India. Similar restriction is also imposed by the insurance sector regarding customer information. All these extra data protective measure will continue to be in existence even if the Government notifies the list.

Exemptions provided under the DPDP Act, 2023

While Section 16 provides for the groundwork layer of governance of cross border data flow by providing a country specific data protection, Section 17 of the DPDP Act, 2023 provides for the exemptions where these restrictions will not apply in relation to certain processing activities and in such cases personal data may be transferred to another country or outside the territory of India. These activities are not restricted only to the government, the private entities, the business organisations can also avail these exemptions which includes:

(i) Where cross border personal data flow is necessary to *prevent, detect, investigate or for the prosecution of offences under Indian law*, the Indian police office and the investigation and law enforcement agencies are not governed by the restriction imposed in relation to the international criminal investigation or extradition mandates. As mentioned it is not only the

government, the private companies can also utilise this exception when the data needs to transferred with relation to any internal investigation or fraud.[73]

(ii) Where restriction to personal data cannot be imposed if it is necessary for *enforcement of legal right or claim,* where private international law comes into play to enforce legal rights such as property disputes of MNCs or resolve legal disputes such as the matrimonial disputes, immigration cases in other country, financial claims outside India, etc.[74]

(iii) Where restriction on cross border data transfer of personal data will not apply when it is necessary for *processing pursuant to a contract with a foreign entity*, where it is specially designed to the Indian outsourcing industry which primarily deals with non-Indian personal data for the processing of their foreign clients.[75]

(iv) Where the cross border transfer of personal data is necessary for the *compromise or arrangement or amalgamation or merger or reconstruction by demerger or undertaking or division of companies,* where any Indian entity who enters into any arrangement with the foreign company may avail this exemption where there will be no restriction on the data regarding transfer of employee information and other personal data to such foreign company but the provision also imposes a duty that such mergers, demergers or any arrangement between the companies should be approved by the court or any other competent authority.[76]

(v) Where the cross border transfer of personal data is necessary for processing to *ascertaining financial position and assets and liabilities of any defaulter by the financial institutions*. These financial institutions may be national, international or private banks or private finance companies, etc.[77]

(vi) Where the restriction on cross border personal data flow will not apply when it is necessary for the *performance of regulatory, supervisory or judicial or quasi-judicial*

[73] Section 17 (1)(c) of the Digital Data Protection Act, 2023
[74] Section 17 (1)(a) of the Digital Data Protection Act, 2023
[75] Section 17 (1)(d) of the Digital Data Protection Act, 2023
[76] Section 17 (1)(e) of the Digital Data Protection Act, 2023
[77] Section 17 (1)(f) of the Digital Data Protection Act, 2023

functions. Regulatory authorities can enforce cross-border enforcement, regulation or supervision even in the countries where it is blacklisted and data should not flow.[78]

In addition to the above exceptions, the act under Section 17(2) provided for another exception where the government can exempt processing (and potentially transfers) for government 'instrumentalities' if it pertains to India's sovereignty, integrity, security, foreign relations, public order, or preventing the incitement of a cognizable offense. Additionally, processing necessary for research, archiving, and statistical purposes is exempt, provided the data is not used for making decisions about individuals and adheres to government-prescribed standards.

Shortcomings of the Act

One of the main drawbacks of the Act is considered to be the uncertainty regarding the blacklisting of countries by the Central Government or provide basis for the permitted data transfers. The act is silent about both the requirements. Even though, the present Act is said to be little restrictive than comparing to the other previous bills, this uncertainty is being a barrier to the cross border data flow. This proposal also creates regulatory uncertainty which provides for non-transparency in the investment field resulting in less foreign direct investments, the investors are also in a confusion about investing in India due to the lack of the guidelines surrounding data transfer. Considering a similar data protection framework which is also principal based like the General Data Protection Regulation (GDPR) of European Union, the provisions are very clear about the requirement of data transfer which is data transfers are permitted to any country or territory which provides a level of protection that is sufficient where the word sufficient is interpreted as equal protection provided by EU to protect the personal data of EU residents. Thus, data transfers are allowed to countries that the European Commission think deemed to provide an adequate level of protection under Article 45, or between entities in jurisdictions that adhere to binding corporate rules under Article 47 or appropriate safeguards under Article 46. These provisions outline the principles for assessing the permissibility of cross-border data transfers.

On the other hand, if you take the data protection law of India, that is the DPDP Act, it offers no such basis or criteria or principles to determine the countries to which data can be

[78] Section 17 (1)(b) of the Digital Data Protection Act, 2023

transferred or cannot be transferred. Till now, the Act only states that the countries will be listed and no list has been published by the Central Government till now. There is also no clarity about what will be factors that will be considered by the Central Government in preparing this list, the Central Government must not show any discrimination among countries while preparing the list and unless there are no definite certain rules, there is no any obligation on the part of India to provide any justification or offer any other alternative mechanism which will be considered to be equivalent to the standard contractual clauses or binding corporate rules through which the data transfers may be permitted to the business and private entities even though the country is located in prohibited jurisdictions.

Additionally, concerns are also surrounding the overriding effect of the sectoral laws restrictions which makes the DPDP act superfluous. There are no provisions in the act to govern the restrictions imposed by the sectors making them the superior authority and complete autonomy regarding the restriction of cross border data imposed by the sectoral laws. The sectoral laws at times issue a higher restriction or higher level of protection than that is necessary which results in a lot of economic implications and economic setback to the country. The act allows such higher restriction without governing them and not considering whether they are necessary or not. The other major setback is that the act by the name itself it can be found that it governs and provides a foundation for only the personal data protection and localisation. A similar framework for non-personal data is still lacking. The non-personal data have a much economic value to it and governance and transfer of such data across borders will provide economic incentives to the Government of India and also to its citizens.

The act provides immense power to the Central Government including a wide scope of discretionary powers regarding the listing of countries and provide data localisation measure which poses potential risk and threats to the privacy and innovation, and enabling arbitrary surveillance. The DPDP Act gives primary focus only to the personal data protection and does not consider the economic impact or the restriction of technology transfer or innovation which results in economic loss to India. Even in the exemptions provided, the Act does not address any economic conditions or the transfer of knowledge like the Intellectual Property as an exception for which cross border data flow may be allowed which results in profit to the country. Fundamentally, India's data policy approach to the cross border data flow or transfer should be a balancing act balancing both the need for citizens to protect their data and not being exploited by the Non-Indian or foreign entities and economic necessity of interacting with other

countries with other countries and global tech firms to sustain economic growth. Unfortunately, the Digital Personal Data Protection Act, 2023 failed to achieve this balance.

To address these shortcomings, an amendment to the Act may be not sufficient as an amendment cannot bring all the guidelines and principles which are compulsorily necessary to support the Act as the act does not address any guidelines on the working of data fiduciary and significant data fiduciary or the guidelines that the private and business entities needs to comply for their obligations under the Act. An amendment may not be even sufficient to address the guidelines or the ground rules that the governments are going to follow for the standard of blacklisting the countries and ensure that there is no any discrimination among the countries in the selection process. Hence a subordinate legislation or rules are absolutely necessary to address all the shortcomings of the act and support the act fully for its better implementation and for the better governance of the data protection in India.

Chapter 4: Data Localisation as an Alternative

Data localisation is considered to be one of the most complex and challenging issue in the context of digital trade or cross border data flow.[79] Data Localisation generally mandates that data pertaining to a particular citizen of a country should be processed and/or stored only within the territory of the country. Chander and Le has defined data localisation as *"any measure 'that specifically encumber(s) the transfer of data across national borders"*.[80] In the context of legislative proposal by the European Commission on cross border data flow, data localisation is defined as *"any obligation, prohibition, condition, limit or other requirement' contained in the 'laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing requirements in the territory of a specific Member State or hinders storage or other processing of data in any other Member State"*.[81] Data localisation can take place in two broad forms. Localised data hosting where the hosts are compelled to store data of the users within the territorial jurisdiction of the country and other one is localised data routing where service providers are under obligation to route data packets between the users by the network located within the geographical jurisdiction of a country. There are mainly two types of data localisation as well:

(i) **Absolute Data Localisation** is when the data should not be transferred across the border at any cost even for any temporary means. When an absolute data localisation is in place, all the data should be collected, processed and even stored within the territory. Hence, cross border data flow is not possible in case of absolute data localisation.

(ii) **Relative Data Localisation** is when a data will be permitted to be transferred beyond its territory but only under predetermined set of conditions either imposed by policy or domestic regulations. This is the most practiced form of data localisation and unlike absolute, relative data localisation allows for cross border data flow but business entities seeking such transfer must follow significant regulations. One example can be the mirroring of data, where one copy of data must be stored locally and other can be used to transfer.

---

[79] See, eg, Antonio Garcia Martinez, 'The End of Data Without Borders' (1 February 2018) The Wired (online); Konstantinos Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) Journal of Cyber Policy 355.
[80] Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64 Emory Law Journal 677, 680.
[81] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union, Doc no. 2017/0228 (COD) (13 September 2017) art 3 (5)

Apart from above-mentioned definition and types, data localisation can also take part in various forms such as explicit data residency policies which asks the data to be stored[82] and/or processed[83] in domestic servers and clouds,[84] and it may also impose that such data should be routed within the territory during the transition,[85] also fall within the scope of data localisation. Further data localisation measure also includes the cross border data flow restrictions on the ground that such restriction is necessary for privacy or data protection,[86] cybersecurity[87] and law enforcement[88] and could force localisation measures by imposing regulatory requirements through policies or unreasonable compliance cost.

The concept of data localisation started in the minds of governments when there were concerns about protection of privacy of individuals especially for the data that is processed or stored outside the territory. As a measure to prevent any breach of data or violation of fundamental right of privacy, these localisation measures were implemented by the governments. The concept of data localisation also gave the idea that the government can have a better control and governance over the data processing, access and transfer if the data is located within the country's borders. In addition to this, governments also believe that domestic laws and regulations can be easily enforced or regulated when the data is stored locally. Examples can be compliance with the domestic privacy law or data access by governments from private entities for criminal investigations, etc.[89] It is also stated that data localisation will

[82] See, eg, [Federal Law No. 242-FZ of July 21, 2014 on Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Data Telecommunications Networks] (Russia)

[83] For example, in the European Union ('EU'), data storage includes data processing. See W Kuan Hon et al, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud' (2016) 24 International Journal of Law and Information Technology 251, 259.

[84] Sometimes, a data localisation measure may not prohibit cross-border transfer although it may necessitate localisation. See, eg, Russian Data Localisation Law. See also Lee Tuthill, 'Cross- border Data Flows: What Role for Trade Rules?' in Pierre Sauvé and Martin Roy eds, Research Handbook on Trade in Services (Elgar, 2016) 357, 363.

[85] For example, a Schengen routing plan was proposed by Germany requiring all personal data of EU residents to be only routed through the EU. See Philipp Bank, 'Deutsche Telekom: "Internet Data made in Germany Should Stay in Germany"' DW: Made for Minds (online), 18 October 2013

[86] See eg Regulation 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, Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119 (1 May 2018) ('GDPR'). In this paper, I use privacy and data protection interchangeably, particularly while referring to legislative frameworks

[87] See eg, Jack Wagner, 'China's Cybersecurity Law: What You Need to Know' on The Diplomat (1 June 2017)

[88] See generally Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64 Emory Law Journal 677, 730-4; Martina F Ferracane, 'Restrictions to Cross-Border Data Flows: A Taxonomy' (ECIPE Working Paper no 1/2017, European Centre for International Political Economy, November 2017) 6.

[89] See generally Shin-yi Peng and Han-wei Liu, 'The Legality of Data Residency Requirements: How Can the TransPacific Partnership Help?' (2017) 51(2) Journal of World Trade 183, 199. See also Alan Mcquinn and Daniel Castro, 'How Law Enforcement Should Access Data Across Borders' (Information Technology and Information

also significantly increase the number of transfers within the country. With the digitalisation, data is considered to be a highly valuable resource to a country[90] and so several countries are increasingly trying to confine such data within their borders to increase their economic profits[91] through these data localisation measures. The economic benefits include attracting investments to the domestic data services, increasing innovation and creating competitive advantage for domestic companies. From the incident of Snowden revelations in 2013 which exposed massive digital surveillance of the US government, several countries started to implement data localisation as a measure to protect the national sovereignty including the national security through cybersecurity and also for preventing breach of data through foreign surveillance.[92] In practicality, many countries might have multiple policy considerations behind these data localisation measures conveniently hiding their protectionist view of supporting the domestic business entities behind the legitimate public policy of data localisation measures.[93]

Part A: Impacts of Data Localisation measures

Data localisation has both positive and negative impact on a country implementing it. These measures may directly or indirectly affect the economy and provide in either an economic profit or economic setback based on several factors. Proponents of data localisation who are in support of it argue that free flow or cross border data flow is being a hinderance to the new pathways of growth. The current digital trade and data regime rely largely on the extensive collection, processing and storage of data for digital surveillance of the users in the south by the global corporations in the north.[94] Thus, in order to create a balance between the south and north and to sustain the power of digital intelligence, developing countries must

Foundation, July 2017) 1, 2; W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 48-9. For historical discussion on this issue, see David R Bender, 'Transborder Data Flow: An Historical Review and Considerations for the Future' (1988) 79(3) Special Libraries 230-235

[90] 'The World's Most Valuable Resource is no Longer Oil, but Data' (6 May 2017) The Economist (online).

[91] See eg, Communication from the African Group, 'Work Programme on Electronic Commerce, Report of Panel Discussion on 'Digital Industrial Policy and Development', WTO Doc JOB/GC/133 (21 July 2017).

[92] Susan Aaranson, 'Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security' (2015) 14(4) World Trade Review 671, 674, 682-5; Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' (Paper presented at Conference on the Future of Cyber Governance, he Hague Institute for Global Justice, 1 May 2014).

[93] See Neha Mishra, 'Data Localization Laws in a Digital World' [2016] Public Sphere 136, 144-51

[94] Gurumurthy, A., Vasudevan, A., &Chami, N. (2017). The grand myth of cross-border data flows in trade deals. IT for Change.

implement interventional state policies to promote domestic over foreign data platforms.[95] Further financing and investing in an 'Internet Plus' digital industrialisation strategy in the areas of big data, cloud computing and Internet of Things will enable the smaller enterprises especially the MSMEs to build their presence online.[96] Countries who also implement data localisation measures on the ground of privacy also argue that it is the only option available to them to protect the privacy of their citizens in the absence of any extensive data sharing treaties between countries.[97] Data localisation is also considered as a response to the broken Mutual Legal Assistance Treaty (MLAT) regime that enables the law enforcement agencies (LEAs) access to data for their criminal investigations and proceedings.

But on the other hand, several economists and legal researchers also argue that data localisation has several economic implications and is a modern day trade barrier especially in the digital trade. Data localisation will be a disturbing factor in the core architecture of Internet of Things especially with regard to Artificial Intelligence. Where the countries have mandated localisation measures, data providers may have to route through networks located only in the territorial jurisdiction making it more congested and affect the overall systematic efficiencies of data providers. Cutting down of data flow or making the cost of cross border data flow higher will not only affect the foreign or multinational entities[98] but also be a hinderance to the domestic firms to participate in the global competition by suppressing their growth and ability in the long run.[99] Moreover, data localisation measures imposed on the ground of privacy, data localisation will only centralise the data making it more vulnerable and susceptible to data breaches and cyber-attacks and it also prevents from incorporating improved security measures like 'sharding'.[100] It is also argued that data localisation will also be an impend to the innovation and will affect the consumers' access to the services and quality of such services. With respect to foreign surveillance, countries may have scale and potential of surveillance capabilities with better security levels at the international level and the better way to protect the data is not to

[95] Ibid.
[96] Ibid.
[97] Panday. Jyoti. Rising Demands for Data Localisation a Response to Weak Data Protection Mechanisms, Electronic Frontier Foundation, 2017
[98] UNCTAD, 2016, Data protection regulations and international data flows: United States International Trade Commission (USITC), Digital Trade in the U.S. and Global Economies, Part 1 (Washington, DC: USITC, July 2013)
[99] IAMAI-IMRB (2017). Digital Commerce Report
[100] Sharding is a process in which rows of a database table are held separately in servers across the world in such a way that shards provide enough data for operations but does not suffice for the re-identification of the individual.

have the same connected to the internet[101] than store it in a country which will only degrade not improve the data protection in that country.[102] The detailed analysis on the positive and negative impacts of the data localisation is discussed below.

Positive Impacts of Data Localisation

Data localisation helps the government in easy monitoring of the data of its citizens, easy monitor of local servers and also helps in taking actions against the operators or business entities for data breach or cybersecurity issues or any such activity which affects the national security. Considering the international co-operation provided in this area, it is likely to implement data localisation measure for tracking down violations or pursuing civil/criminal action against violators as it is easy to do so in one's territory than comparing to action against companies who operates and provide services from abroad. Further more data localisation can also be justified on the ground of privacy and data protection if a country is preventing the transfer of data to countries with very less or weak data protection and cybersecurity. Unless there is an international law in this regard of data protection and privacy of individual, it is safer to store the data in its own territory for better supervisory than allow a cross border data flow.

Any other alternative measures of data protection and privacy is either not reasonably available to the country due to its inadequate regulatory capacity or that it does not provide the same or equivalent level of cybersecurity and privacy protection that data localisation does. Many experts have argued that accountability approach in data protection will be more viable than a data localisation measure.[103] However, in practicality, a provision or policy in accountability approach making the digital service providers liable is ineffective by itself. For example, monitoring or auditing of all the data processing facilities provided by the digital service providers which even includes cloud storage is not possible even for developed countries. Furthermore, when the chances of getting caught is negligible in a host country due to its poor executive measures, the foreign digital service providers are more likely to only

[101] Chander, Anupam, and Uyên P. Lê. "Data nationalism." Emory LJ 64 (2014): 677.

[102] Hill, Jonah. "The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders." In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance. 2014.

[103] W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 221. See generally Colin L Bennett, ' The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Daniel Guagnin et al eds, Managing Privacy through Accountability (Springer online, 2012) 33.

avoid the excessive data protection that is implemented by the domestic legislation even though they are binding on the service providers which results in less data protection available to the citizens of that country and are more vulnerable to cyberattacks or cyberbreaches.[104] Hence an accountability approach may be a useful component of strict data privacy but it does not provide protection equivalent to that of data localisation.

Data localisation can help a country in a number of economic ways. These economic activities include investing in the domestic servers by the foreign entities, increasing the data activity of the domestic country including a significant increase in the transfer, etc. This is even backed by evidence of a 2018 report commissioned by Facebook. According to the report, Facebook has set four data centres in the U.S. which alone contributed a cumulative $5.8 billion to the U.S. economy between the years 2010 and 2016, an amount which translates to "$835 million per year.[105] A large portion of this contribution was because of the upfront capital investments for the construction of data centres which alone contributed to 82 percent.[106] Hence this supports the fact that presence of data centres in a country will bring significant economic benefits to a country. The presence of data centres not only brings the economic benefits to a state but also provide an efficient and a quality cloud services to the local users in the form of improved latency, meaning reduced time for the movement of data packets from source to destination.[107]

Negative impacts of Data Localisation

Several researchers have conducted studies which shows that there are disruptive economic impacts of data localisation and it is considered to be a threat and hinderance to the trade in digital economy.[108] Complying with the data localisation measures, countries are

[104] See generally Dan Jerker B Svantesson, 'The Regulation of Cross-Border Data Flows' (2011) 1(3) International Data Privacy Law 180, 194.
[105] Zachary Oliver, Kyle Clark-Sutton, Sara VanLear, Lindsay Aramayo, and Brian Lim et al., "The Impact of Facebook's U.S. Data Center Fleet," RTI International, March 2018, https://baxtel.com/data-center/facebook/files/ facebook_data_centers_2018.
[106] Ibid.
[107] While announcing its new cloud platform region in Mumbai, Google declared that this would improve latency from 20 percent to 90 percent for end users in certain Indian cities compared to hosting these services in Singapore, which was the closest region. See Dave Stiver, "GCP Arrives in India With Launch of Mumbai Region," Google Cloud, November 1, 2017, https://cloud.google.com/blog/products/gcp/gcp-arrives-in-india-with-launch-of-mumbai-region.
[108] See eg, Matthias Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (ECIPE Occasional Paper 3/2014, 2014); Joshua P Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (2014) 2 Asia & the Pacific Policy Studies 90, 92; United States International Trade Commission, 'Digital

forcing business entities to store data locally which affects the core infrastructure of the Internet of Things and disrupts the technological and commercial arrangements which are inherent to the digital sector in its built, thus affecting the economy of a state since majority of the entities rely on economies of scale in digital sector.[109] One best example is the working of the Artificial Intelligence and blockchain technologies. Artificial intelligence collects data across the globe and if the data input is cut to the artificial intelligence, its accuracy in the output is likely to be very low. Further, a foreign service supplier or global value chains will not be willing to relocate their servers to a country with poor regulatory or which lacks physical infrastructure.[110] This will only increase the compliance and operational costs for these foreign service providers as they will be forced to either built their own local servers or use the local services offered by domestic entities in all implementing countries. Smaller companies who operate outside the country might lack the financial capacity to build servers and hence they may be prohibited from entering the market because of data localisation laws. All these factors signifies that data localisation measures are an overall hinderance to the international trade as it significantly reduces the exports by foreign service providers.

Data localisation also disrupts the network economies of scale.[111] For example, companies who were efficiently managing data distribution through continuous back-end transactions across various global/regional servers, companies are now required to synchronise and process the data distribution within fewer domestic servers located within the territory which will increase the risk of overloading of data at a particular server and security breaches.[112] Apart from this, companies also face a significant increase in the transaction and transmission cost to comply with stringent and restrictive standards of privacy or data protection that disrupts the interconnectivity across the global value chains.[113] In addition to this, the extensive data protection laws and policies with mandates consent from the individuals

Trade in the US and Global Economies, Part 2' (Publication No 4485, August 2014) 65; James Manyika et al, 'Digital Globalization: The New Era of Global Flows' (McKinsey Global Institute, March 2016)

[109] W Kuan Hon et al, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud' (2016) 24 International Journal of Law and Information Technology 251, 253-54.

[110] James M Kaplan and Kayvaun Rowshankish, 'Addressing the Impact of Data Location Regulation in Financial Services' (Global Commission on Internet Governance, Paper Series no 14, CIGI and Chatham House, May 2015) 1.

[111] Iva Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?' (2016) 50 (2) Journal of World Trade 313, 317-19; W Kuan Hon, Data Localization Laws and Policy (Edward Elgar, 2017) 112- 114; Leviathan Security Group, 'Quantifying the Costs of Forced Localization' (2015)

[112] Richard Bennett, 'Surge in Data Localization Laws Spells Trouble for Internet Users' on TechPolicyDaily.com (10 May 2016)

[113] Iva Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?' (2016) 50 (2) Journal of World Trade 313, 317-19

for every individual users and/or appropriate authorities for use/processing or transfer of data like the data protection law in India also increase the compliance cost to the business entities.[114] Additionally, domestic companies that rely on digital services, along with end consumers, face limited access to competitive foreign services, resulting in a loss of significant business and other opportunities.[115]

From a technological perspective, the geographical points on data flows and data location shrinks and disrupts the end-to-end architecture which requires unbothered and instantaneous flow of data across the network servers, irrespective of where the data is collected or processed which is the point of origin or content of data.[116] Further, in the modern day technology companies and business entities use autonomous data routing which is done automatically through computer codes and underlying technical protocols and because of this, data move through the most efficient route between the users rather than aligning with the territorial boundaries.[117] Thus, data localisation artificially disrupts the technical and logical infrastructure of the internet, undermining its reliability as a platform for data transfer.

From the perspective of economic efficiency, it is evident that data localisation provides undesirable consequences for all the stakeholders in a country which includes business entities, governments and even consumers. As mentioned earlier, it increases compliance cost for business entities. For government, monitoring of the domestic data providers whether they are complying with the data policies and regulations needs a regulatory authority or board and it efficiently increase the resources[118] to achieve the data protection which is also considered to be an impractical outcome because data will travel instantaneously from one server to another of multiple locations in the world within a blink of eye, so it is impossible to track the exact location of data in real time points[119] and instantaneously proves that the end goal of data

[114] See eg, GPPR, art 6-9, art 22.
[115] Iva Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?' (2016) 50 (2) Journal of World Trade 313, 317-19; W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 112-114.
[116] Simson Garfinkel, 'The End of End-to-End?' (1 July 2003) MIT Technology Review (online); W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 32, 105.
[117] R Barnes et al, Technical Considerations for Internet Service Blocking and Filtering, RFC 7754, Internet Engineering Task Force (March 2016) 12.
[118] Lexology, Russia's Personal Data Localization Law: Expanding Enforcement (27 April 2016); Hogan Lovells, 'Russia Releases 2017 Data Privacy Inspection Plans; Microsoft Passes 2016 Inspection' (19 January 2017)
[119] W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 100; Tatevik Sargsyan, 'Data Localization, and the Role

protection and privacy is not dependent on the location of data rather it is dependent on the underlying technical protocols and designs used by the digital service providers.[120] For example, if an encryption mechanism used by a data provider is weak, privacy of individuals may be affected irrespective of location of server and the same applies when the cloud service stores data, if it does not provide robust defence mechanisms, it is very vulnerable to cyberattacks affecting privacy and data protection even if such a cloud server is located within the country. On the other hand, the foreign entities may use end-to-end encryption for protection of data and robust security for cloud services for storing of data outside the territory providing more protection. For consumers, since the compliance cost increases for the business entities, it might result in increased price[121] for the end consumers and these consumers may also not be provided with all technological services due to the limited capacity of the domestic servers.

Even with handful of evidences showing that data localisation measures are economically insufficient and even disruptive in nature, there is still a rise in the number of policy communities implementing such measures particularly since the year 2013.[122] These communities are mostly the internet technical and policy community comprising various multi-stakeholder organizations involved in internet governance;[123] trade institutions such as the

of Infrastructure for Surveillance, Privacy and Security' (2016) 10 International Journal of Communications 2221, 2221.

[120] Tim Maurer et al, 'Technological Sovereignty: Missing the Point?' in M Maybaum et al eds, Architectures in Cyberspace (NATO CCD COE Publications, 2015) 53, 61-2; Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers and What Do They Cost?' (May 2017) 3-4; Konstantinos Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) Journal of Cyber Policy 355, 361-2; United States International Trade Commission, 'Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions' (Publication number 4716, Investigation Number 332-561, August 2017) 285; Usman Ahmed and Anupam Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows' (Think Piece, E15 Expert Group on the Digital Economy, International Centre for Trade and Sustainable Development and World Economic Forum, November 2015) 6-7

[121] See Matthias Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (ECIPE Occasional Paper 3/2014, 2014).

[122] Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' (Paper presented at Conference on the Future of Cyber Governance, The Hague Institute for Global Justice, 1 May 2014).

[123] The internet technical and policy community consists of organisations such as Internet Governance Forum ('IGF'), Internet Engineering Task Force ('IETF'), World Wide Web Consortium ('W3C'), Internet Corporation for Assigned Names and Numbers ('ICANN') and Internet Society ('ISOC')). Further, civil society organisations and technology companies are also often active members of the internet governance community, participating through several of the above bodies. See, eg, discussion at IGF 2017 on 'Digitalization and International Trade' (19 December 2017)

WTO;[124] human rights bodies;[125] and several governments, particularly digital leaders like Japan and the US.[126] Recurring concerns against data localisation include the fragmentation of the global internet into inefficient, localized networks;[127] the rise of digital protectionism, which reduces economic opportunities and productivity;[128] and an increase in online surveillance and oppressive censorship.[129]

Part B: Data Localisation measures in India

While data localisation measures have been a topic of intense debate recently, its implementation by India is certainly not new. The Public Records Act (1993) and the security conditions implemented under the Unified Access License for Telecom Services (2004) are earlier examples of data localisation measures by India. These measures were implemented to protect and safeguard the sensitive data. The Public Records Act, 1993 imposes the prohibition that transfer of public records outside the territory of India. Such transfer under the Act was only permitted for a social purpose to protect the sovereignty and integrity of India or with the permission of the central government.[130] Similarly, IT Regulations under the IT Act with its amendment in 2008 and Rules in 2011, limited the transfer of sensitive personal data by a body corporate or business entity to another body corporate or person, who resides or situated outside the territory of India but exception was provided that if such entity or person provides an equivalent level of data protection then the data maybe shared under the IT rules. There were two pre-conditions to it that only if such transfer is necessary for performance of existing

[124] See discussion of electronic commerce at the WTO in Daniel Crosby, 'E-commerce and Digital Trade for Development: Negotiations to Soft Launch at MC11' on E15 Initiative (October 2017)

[125] See, eg, Kinfe Michael Yilma, 'The "Right to Privacy in the Digital Age": Boundaries of the "New" UN Discourse' (2018) 87(4) Nordic Journal of International Law 485-528 (discussing the UN General Assembly resolutions on digital privacy). See also Access Now, 'The Impact of Forced Localisation on Human Rights' (4 June 2014) <https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/ >. See also Anupam Chander, 'International Trade and Internet Freedom' (2009) 102 American Society of International Law Proceedings 37.

[126] WTO, Work Programme on Electronic Commerce - Non-paper from the United States, WTO Doc JOB/GC/94 (4 July 2016) [2.3]; WTO, Work Programme on Electronic Commerce - Non-Paper for the Discussions on Electronic Commerce/Digital Trade from Japan, WTO Doc JOB/GC/100 (25 July 2016) [2.2].

[127] See generally William J Drake et al, 'Internet Fragmentation: An Overview' (Future of the Internet Initiative White Paper, World Economic Forum, January 2016); Global Commission on Internet Governance, 'One Internet' (CIGI and Chatham House, 2016).

[128] See eg, WTO, Work Programme on Electronic Commerce - Non-paper from the United States, WTO Doc JOB/GC/94 (4 July 2016); WTO, Work Programme on Electronic Commerce - Non-Paper for the Discussions on Electronic Commerce/Digital Trade from Japan, WTO Doc JOB/GC/100 (25 July 2016).

[129] Tatevik Sargsyan, 'Data Localization, and the Role of Infrastructure for Surveillance, Privacy and Security' (2016) 10 International Journal of Communications 2221, 2221.

[130] See Section 4 of the Public Records Act 1993

contract and the individual has consented for the same. Further, for all the entitles to which Companies Act, 2013 is applicable, a back-up of books of accounts and other books and papers of the company which are maintained in an electronic mode, including any records that are kept or stored outside India, must be periodically stored in the servers physically located in India.[131]

Similar to this, there were governmental policies which also implemented data localisation measures such as the MeghRaj initiative, launched by Government of India in 2014 which imposed data localisation by proposing a pre-condition that to be an empanelled cloud service provider to the government, data must be located only in India. The National cloud service was started with the aim of promoting the use of cloud computing to accelerate the delivery of government e-services and optimise the government's ICT spending.[132] Localisation measures were also implemented in Draft National E-commerce Policy. In February 2019, when the revised version was announced, the policy imposed restrictions on the cross border data flow of the data collected by IoT devices which are installed at the public places and the policy also governed the data generated by Indian users on Internet platforms such as e-commerce, social media, search, etc.

Apart from these, there were also several sectoral policies which has preceded the data privacy protection of India also implemented data localisation in India by directly or indirectly regulating cross border data flow. It is the telecommunications and the finance department who holds a large volume of data and hence they came with several policies. The most prominent data localisation measure was the RBI's notification on localising the payment systems data inside India. The RBI under the Directive on Storage of Payment System data, 2018 has stated that all data relating to payment transaction should be stored in a system located only in India. A note of caution was raised that the RBI Directive on the localisation of payments data could undermine fraud detection systems and the identification of money laundering within the domestic payments system. The Directive mandated that payment companies store the data of Indian users exclusively on local servers and remove any back data from global servers. This directive faced criticism from industry stakeholders due to the absence of a proper consultation process and a lack of clarity on various compliance aspects. In response, the RBI clarified that

[131] "The Localisation Gambit". The Centre for Internet and Society (2019)
[132] https://cloud.gov.in/about.php

all payments data, including end-to-end transaction details and information related to payment or settlement transactions gathered, transmitted, or processed as part of a payment message or instruction, must be stored only in India.

In the insurance sector, the Insurance Regulatory and Development Authority has also implemented that data in relation to policy holders' records should be maintained in India. In the telecommunication sector, the telecommunications and internet service providers who holds the Unified Access License are strictly restricted from transferring or storing user information regarding their personal details or accounting information who are their subscribers outside the territory of India except for International billing.[133] In the broadcasting sector, the Consolidated Foreign Direct Investment Policy, 2020 has implemented a pre-condition to the foreign direct investment that Foreign direct investment is subject to the condition that "the company shall not transfer the subscribers' databases to any person/place outside India unless permitted by relevant law. The degree of restrictions differs by sector. For instance, payments data must be stored locally, while e-Pharmacy regulations and critical personal data are generally prohibited from cross-border transfers, with few exceptions. The e-commerce policy permits cross-border data flows but requires a copy of the data to be stored within the country. The economic impact of these policies will depend on various factors, such as the size of the entity, the business model, and the sector of operation.

Even though there are several sectoral policies, the general law which governs data localisation in India is the Digital Personal Data Protection Act, 2023. It imposes a localisation measure in Section 16 by stating that no personal data shall be transferred outside the territory of India except under the circumstances provided in Section 17. There is no comprehensive law which governs non-personal data and government data, hence these data are still governed by the sectoral policies.

Economic Implications

Several studies and evidences have shown that the cost of data localisation will impact the Indian economy especially this impact is highest for the sectors such as communication and financial services.[134] The financial service providers in the industry is a mix of both domestic

[133] Bailey, Rishab, and Smriti Parsheera. "Data localisation in India: Questioning the means and ends." NIPFP Macro/Finance Group (forthcoming) (2018).
[134] Ibid.

and foreign entitles in India and their global services are therefore subject to the localisation mandates. For example, in the credit card industry, it could impact the ability of these financial service provider companies to share data across third-party operators outside India on credit history, transaction data, etc. which helps the entities or officers to identify frauds and co-ordinate remedial actions.

Few companies, in the anticipation of these data localisation measures especially the start-ups have moved their data to cloud services in India. Since majority of these start-ups are typically dependent on the external funding of investment and have tight cash flow, the additional compliance cost has been burdensome for these companies which prevented them from entering the market. One such example is a communication app company of foreign origin with one of its largest markets is in India, in a report it stated that it has to maintain two data centres now out of which one is in India due to the localisation measure and the company stated that as an added burden to the already cost. Similarly, another US based social enterprise which was working on the health and technology department has developed projects for the Government of India, was under an obligation to store their data on National Informatics Centre (NIC) servers in India. Later, these data were moved to the private sector in India for better compliance. Even though, the company had a data server in US, it was forced to build and maintain one in the territory of India. The draft of the e-commerce policy was also heavily criticised when it was introduced.

The Ministry of Electronics and Information Technology (MEITY) refused to accept that the proposed e-commerce policy which attempted to prescribe rules on data management in many ways, it overlapped with the comprehensive framework of data protection which was emerging at that time. The issue was discussed with the Ministry of Commerce and Industry and was sorted later. The 2019 National Trade Estimate Report on Foreign Trade Barriers by the US Trade Representative reportedly stated that the India's new data localisation measures would act as a significant barrier to the trade in digital economy between India and U.S. Moreover, the data localisation policy which supposedly introduced to encourage domestic companies to build competitive advantage is also hurting the small and medium sized enterprises on account of the compliance cost and also inhibiting from using the cheap foreign services thus affecting their growth in the global market as well.

1 percent (1%) increase in the international internet bandwidth has increased a proportion of International Trade and has increased US$ 696.71 million in total volume of goods trade for India. From the year 2016-17 and from the year 2017-18, international internet bandwidth alone has increased by 35 percent, which lead to an increase of about US$ 24 billion in total volume of goods trade. During this period, India's total trade volume increased by approximately US$ 202 billion. Consequently, around 12 percent of this growth can be attributed to the increase in international internet bandwidth. Similarly, the same report has suggested that a 1 percent (1%) decrease in the cross border data flow will reduce the volume of International Trade by US$ 696.71 million for India. This is only an overall estimation of the total reduction of volume of trade and precise impacts can be established once the nature and volume of restriction are clearly known for each sector. In a practical sense, not all the cross border data flows are going to be personal data or critical data which are potentially impacted by the data localisation measures. Due to this, the data that are not personal and has much commercial value to it is also affected since they have some spill overs to other categories which are sometimes inadvertent.

The impact of data localisation is found to be different for companies in various sectors and it is also evident that it also differs for companies within the same sector as well. The most affecting factor in a data localisation measure is the size of the company. Most small and medium sized companies especially which are of Indian origin and operating in India have reported a one-time cost of migrating the data to servers in India and no recurring cost after the same or no recurring impact from the data localisation. In the short to medium sized entities, these companies might have compromised their quality of services and may contented with the existing quality of service available at data servers in India. On the other hand, the multinational companies and global service providers scaling up their services in India, they are very well known for their quality of service and they will not compromise any decrease in quality and so the local data centres will have to eventually match up their overseas counterparts. A small foreign-owned financial services company operating in India indicated that, in the absence of localisation requirements, it would prefer to store data outside the country. Meanwhile, a social enterprise involved in Government of India projects noted that the government prioritizes storing all information related to social welfare schemes and initiatives within India, even if it results in project delays. This exemplifies the opportunity cost of data localisation, a trade-off the government is willing to make. However, there could be additional unknown and unanticipated costs associated with strict data localisation policies, which might undermine

some of India's comparative advantages in the digital and technological sectors. Even with companies which do not currently involve in any cross border data flow but complying with the data localisation norms has also stated that their preference for storing data is outside the territory of India who provides moderate opportunity costs and better services comparing to the increased cost with the local data service providers.

Part C: Issues at Hand and Recommendations

Having discussed the various regional and international policies and national laws that govern cross border data flow at the international and the national level in India in depth, it becomes necessary to look at what all are the changes that can be brought in them so that the balance between the allowance of cross border data flow considering its economic value to a country and the data protection and protection of privacy of individuals of a state can be achieved. Therefore, firstly, a concise summary of the situation at hand is needed before possible solutions can be come up with. Looking at the same, there are basically four major issues at hand that needs to be addressed.

First, is the consensus over the international policies that govern cross border data flow. Cross border data flow is a concept that cannot be confined to a single state or nation. It involves more than one or more state at a time and hence co-operation is needed among nations but till this date, there is no any comprehensive legal framework at the international level which addresses cross border data flow or there is no any authority to govern the same which led to the formation of many regional policies. There is no uniformity in approaching the cross border transfer of data among the governments. The prescriptive regulatory approach which was largely highlighted by the governments does not align with the multi-stakeholder approach proposed by the experts in the internet technical community as well as the private sector.[135] Even among the regional policies, there is a huge divide which exists on the framework governing cybersecurity and privacy laws and regulations. This can be very well understood by the US and EU backlash against the Chinese cybersecurity law at the WTO[136] which

[135] Several engineers of top technology companies are also members of technical standard setting institutions such as the IETF and W3C, thus showing the close links between the internet technical community and the private sector.

[136] See, eg, Hannah Monicken, 'U.S., China Trade Criticisms at the WTO Over Cybersecurity Measures' (14 December 2018) 36(4) Inside US Trade (online); Communication from the United States, Measures Adopted and Under Development by China Relating to its Cybersecurity Law - Questions to China, WTO Doc S/C/W/378 (3

imposes very stringent localisation and data sovereignty policies and the tensions between the data transfer mechanism of the two major regional co-operations the Asia Pacific Economic Co-operation (APEC) and the European Union (EU) clearly reflects the division between the approaches taken by countries on privacy and cybersecurity issues.[137] Only when the conflicts between these perspectives remain solved, there will be a scope for the international law or policy for governing different standards of data protection and conflicting perspectives on cybersecurity. Because of all these issues in the different approaches, the countries find it convenient just to restrict the data flows through data localisation measures rather than come negotiate to a middle path on data flow. This conflict is even further complicated when governments attempt to export their regulatory approach and models on data protection or cybersecurity to other countries, especially through the preferential or regional trade agreements[138] which causes further fragmentation in the global regulatory framework on data flows.[139]

Second, is whether data localisation is the real answer or solution to the data protection or cybersecurity and protection of right to privacy of individuals. Technical evidence and studies often weigh against the general concept of data localisation measure to contribute towards the cybersecurity and privacy.[140] In the context of cybersecurity, data localisation does

October 2018); Communication from the United States, Measures Adopted and Under Development by China Relating to its Cybersecurity Law, WTO Doc S/C/W/376 (23 February 2018); Communication from the United States, Measures Adopted and Under Development by China Relating to its Cybersecurity Law, WTO Doc S/C/W/274 (26 September 2017); Communication from the European Union, Statement by the European Union to the Committee on Technical Barriers to Trade 20 and 21 June 2018, WTO Doc G/TBT/N/CHN/1172 (9 July 2018). See also United States Trade Representative, National Trade Estimate Report (2016) 91

[137] Lexology, 'APEC and EU Discuss Interoperability Between Data Transfer Mechanisms'

[138] See eg, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (signed 8 March 2018, not in force) ('CPTPP') art 14.8.2 (setting out a broad definition of regulatory framework for protection of personal information including self-regulatory privacy models, prevalent in the US and other APEC countries); United States – Canada- Mexico Trade Agreement ('USMCA')

[139] See generally on electronic commerce provisions in regional trade agreements, Mark Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System' (Overview Paper, RTA Exchange, Inter-American Development Bank and International Centre for Trade and Sustainable Development, November 2017); Jie Huang, 'Comparison of E-commerce Regulations in Chinese and American FTAs: Converging Approaches, Diverging Contents and Polycentric Directions?' (2017) 64(2) Netherlands International Law Review 309.

[140] Tim Maurer et al, 'Technological Sovereignty: Missing the Point?' in M Maybaum et al eds, Architectures in Cyberspace (NATO CCD COE Publications, 2015) 53, 61-2; Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers and What Do They Cost?' (May 2017) 3-4; Konstantinos Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) Journal of Cyber Policy 355, 361-2; United States International Trade Commission, 'Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions' (Publication number 4716, Investigation Number 332-561, August 2017) 285; Usman Ahmed and Anupam Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows' (Think Piece, E15 Expert Group on the Digital Economy, International Centre for Trade and Sustainable Development and World Economic Forum, November 2015) 6-7

not reduce any network vulnerabilities such as cyberattacks or vulnerabilities to natural disasters or data fraud.[141] As discussed earlier, cyberattacks are mostly dependent on the cybersecurity measures taken to tackle them and not the location of data. On the contrary, localising makes the data less secure only as it becomes concentrated in very specific servers within the country making them an easier target for cyber-attacks and surveillance.[142] Further, governments implement data localisation on account of easy surveillance by them. On the contrary, data localisation does not increase the government access to the data as these data are mostly end-to-end encrypted or encrypted[143] which is followed by the private service providers for the privacy of individual and hence government cannot access these data. Similarly, if multiple governments claim right to a single data[144] it will only enhance the problem. Technical evidence also suggests that data localisation leads to significant engineering inefficiencies. For instance, it disrupts the underlying transfer protocols of the network by forcing data to be routed in specific ways. This interference can cause delays and inefficiencies in data transmission, which are particularly problematic for global digital services that rely on fast and seamless data flow and thereby, disrupting trade in digital services.[145] The territorial logic behind data localisation measures, however, does not align well with the nature of digital data flows, especially in the age of ubiquitous cloud computing.[146] Experts argue that cloud computing allows for the instantaneous and automatic routing of data packets to multiple locations worldwide simultaneously, often through a process called sharding,[147] which breaks data into smaller packets. Therefore, the location of internet users is irrelevant to where or how their data is stored.[148] Consequently, the physical location of the data—whether on domestic or foreign servers, a single server, or multiple servers across different parts of the world—cannot

[141] W Kuan Hon et al, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud' (2016) 24 International Journal of Law and Information Technology 251, 262.
[142] Patrick S Ryan et al, 'When the Cloud Goes Local: The Global Problem with Data Localization' (December 2013) Computer (online) 54, 56.
[143] W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 70.
[144] Ibid 62, 89.
[145] See generally Laura DeNardis, 'Introduction: One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation' in A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability Volume I (Centre for International Governance Innovation and the Royal Institute of International Affairs, 2016) 4, 6-10.
[146] W Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (Edward Elgar, 2017) 32, 105
[147] Jeeyoung Kim, 'How Sharding Works' on Medium (6 December 2014) <https://medium.com/@jeeyoungk/howsharding-works-b4dec46b3f6>.
[148] See Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326, 329

determine the security, quality, or privacy of the data.[149] Instead, it is the robustness of the technical designs and protocols underlying the internet network and digital services that determine data security and privacy.

Third, is the economic complications of the cross border data flow. Even though there are several studies which conclusively states that there is an economic setback if there is a restriction in the cross border data flow, however it is not easy to measure to direct economic impact[150] of cross border data flow as data is very hard to trace among different sectors. Therefore, presenting any solid or robust quantitative evidence of the restrictive impact of data localisation is not always possible for a country.[151] The government also instead of focusing on the quantitative evidence, it should sometimes understand the way how a data localisation blocks the cross border data flow and thus increase the degree of trade restrictiveness. For instance, if a data localisation measure disrupts underlying transfer protocols or the integrity of the domain name system, its trade-restrictive impact is far more significant than if it merely requires a few digital service providers to make minor adjustments to their technical design or terms of use. On the contrary, countries can look into evidence of how much they have been profited from the cross border data flow. Even though, this will not be the same as losses due to restrictions, it gives a rough draft to a country about the economic implications. For example, over the past two decades, India has greatly benefited from open practices that allow free cross-border data flows and the import and export of digital services. According to one study, digital trade generated $35 billion in economic benefits for India in 2019, with projections indicating this figure could rise to $512 billion by 2030, amounting to 10 percent of the country's projected GDP at that time. Even though data localisation brings in lot of economic opportunities such as providing competitive advantage to the domestic data service providers, building of new data centres, employment opportunities to people, etc. All these opportunities does not apply to all countries and countries should have supplementing materials such as policies and investments. Even if considered that a country has all these things, the economic

[149] Dara Hoffman et al, 'Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud' (2017) 10 Algorithms 47, 55-6; Tatevik Sargsyan, 'The Turn to Infrastructure in Privacy Governance' in Francesca Musiani et al eds, The Turn to Infrastructure in Internet Governance (Springer, 2015) 189, 198; Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64 Emory Law Journal 677, 730.

[150] Economics and Statistics Administration and the National Telecommunications and Information Administration, 'Measuring the Value of Cross-Border Data Flows' (US Department of Commerce, September 2016) 1.

[151] Both quantitative or qualitative evidence can be put forth to assess the restrictive impact of a measure. See AB Report, Brazil – Retreaded Tyres [146].

compensation provided will not be as proportional as provided by the cross border data flow to the GDP.

Fourth is the drawbacks in the national laws of India in governing the cross border data flow. First of everything, there is no comprehensive framework or any law or regulation that specifically addresses or governs the cross border data flow. Just like many other countries, even in India it is the personal data protection laws which governs the cross border data flow. There is a default mistake in this as cross border data flow not always involves personal data sometimes or most of the times it is only the non-personal data or the public government data that is shared. India does not have a legal framework for non-personal data. Even though the idea of governing non-personal data was proposed by Sri Balakrishna Committee in the Data Protection Bill, 2019 the government rejected it later stating that it is difficult to separate the personal data from the non-personal data. The problem with privacy laws governing the cross border data flow is that they keep only the protection of privacy and cybersecurity in mind and impose severe restrictions or more restriction than that is necessary which prohibits the cross border data flow.

Recommendations

Since, there are issues regarding the governance of cross border data flow at both the national and the international level, there needs to be policy recommendations at both these levels for the better governance of the cross border data flow. At the national level in India, currently there are loopholes in the Digital Personal Data Protection Act, 2023 as mentioned in the shortcomings of the act and these loopholes needs to be addressed for the better governance of the cross border data flow. It is highly recommended that the government should come up with Digital Personal Data Protection Rules or a subordinate legislation that supports and clarifies the Act and addresses the issues of the Digital Personal Data Protection Act, 2023. While enacting such rules or subordinate legislation, the government should consider these principles which helps in bridging the gaps in the Act. They are

(i) Non-discriminatory Treatment: First, the government should not show their own interest and the government should not discriminate among countries when deciding whether to place them on the blacklist. "There must be well-defined rules in determining the blacklist based on which it would deny data transfers to certain regions/countries to ensure uniform

treatment has been given, including criteria for consent mechanisms, transparency, accountability, and all other aspects, especially for cross-border data flows,". It is also important to consider other countries' laws to ensure non-discrimination and compliance with the same. For instance, reference can be given to the Schrems II judgment in the EU. "In that case, the Court of Justice of the European Union invalidated the privacy shield between the EU and the US because of the fact that the US had certain surveillance programs that did not adequately protect EU citizens' data according to the required adequacy standard provided under the General Data Protection Regulation (GDPR). Hence, it was invalidated. Therefore, it is absolutely necessary to establish foundational norms based on existing practices in other countries and set our standards accordingly, ensuring they are practical and easily operationalized,".

(ii) Data responsibility: Cross border data flow and privacy protection is also dependent on Data responsibility which involves the due diligence requirements that companies must adhere to. "Under IT Act and its rules, there are numerous obligations for data fiduciaries and intermediaries. Similarly, we should have similar due diligence requirements for data fiduciaries and significant data fiduciaries under the DPDP Act as well,". Even though there are mentioning of the same in the Act, it is not comprehensive enough as it lacks guidelines that needs to be followed by these data and significant data fiduciaries.

(iii) Data localisation: Even though data holds such an economic value to it and cross border data flow should never be restricted, the protection of privacy of individuals should also be considered on the other hand. Hence, even though data localisation brings in economic implications, there should be a partial data localisation. For this, the first and foremost action the Indian government should take is categorizing data, which is currently missing from the Act. Even though in the previous bills, there were categorization of personal data into sensitive personal data and critical personal data, the present Act does not categorize any data. For data localisation, servers must be located in India. This requirement should apply only to very sensitive data, specifically critical data and cross border data flow of other data should be allowed.

(iv) Data resilience: The new rules should absolutely focus on the guidelines that the industry in the data sector needs to comply. It is almost the private sector that deals with the data in India and hence a comprehensive rule or guidelines should be framed where the

government will inform the industry about the steps that needs to be taken in the case of any technical failures, cyberattacks or data breaches. The rules should also include steps for having redundancy and backup plans, as well as recovery plans. These industries must also adopt the residency policies of the government.

Hence the government must consider these principles when enacting the digital data protection rules for better addressing of the cross border data flow and the government must also consider the evolving standards of the data policies around the world and should update the rules according to the technological advancements. The government must also not consider blacklisting as a one-time process and should keep on changing according to the circumstances.

Data Free Flow with Trust (DFFT)

At the international level, there is no international co-operation in the policy of cross border data flow. The lack of these effective and trusted policy cooperation mechanisms for the governance of cross border data flow has led lawmakers to seek alternative approaches which resulted in the regional frameworks for cross border transfer. In the name of regional policies, many jurisdictions have introduced discriminatory measures on international data transfers or extended their laws beyond their own territories through trade agreements and other means. Studies have shown that the number of data restrictive policies has doubled over the past decade or 10 years.[152] In this critical time where leaders of international organisations were thinking if the situation is left unnoticed it will destruct the cross border free flow of data, Japan's Prime Minister Shinzo Abe called for international rules suitable for the digital age, which strikes the balance between carefully protecting sensitive data while allowing productive data to flow across borders. In his landmark speech at the World Economic Forum Annual Meeting 2019 in Davos-Klosters in January, Prime Minister Abe urged leaders to establish an international order for **Data Free Flow with Trust (DFFT)[153]**, a vision where openness and trust coexist harmoniously for the free flow of data. Concurrently, 76 countries initiated new negotiations on digital trade, known as the ongoing Joint Statement Initiative (JSI) on e-commerce.[154]

[152] VOX, Centre for Economic Policy Research (CEPR) Policy Portal, "The cost of data protectionism", 2018; World Economic Forum, "Exploring International Data Flow Governance", White Paper, 2019.
[153] Abe, Shinzo, Toward a new era of hope driven economy, 23 January 2019, speech presented at the Word Economic Forum Annual Meeting 2019, Davos-Klosters
[154] World Trade Organization Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.

In June of that year itself, during the G20 Ministerial Meeting in Tsukuba under Japan's chairmanship, trade and digital economy ministers emphasized the importance of cross-border data flows for economic development, social benefits, productivity, innovation, and sustainable development.[155] They also highlighted that to achieve data free flow with trust, there is a need to address challenges such as security, data protection, and intellectual property, which are very crucial for maintaining public trust in digital technologies in the modern times. In other words, "free" flows do not imply a world without appropriate rules or safeguards it means that data will be free flowing within the secured umbrella of protection. The Osaka Track is an initiative to promote international rule-making for data flows with trust. Achieving this will require global cooperation in not only the areas of data flow or data protection but also in the areas such as international trade, laws, regulation, technology, and other aspects of governance, with some both binding and non-binding rules for governments, businesses, and users. So far, governments, industry, and user groups have participated in intergovernmental and multi-stakeholder forums to develop international norms, guidelines, principles, and standards. However, the issue with cross border data flow is that there is no single forum addressing all issues related to global data governance.

The binding and non-binding rules for government may appear to overlap or conflict with one another, but generally, they are complementary in nature, each serving as a pillar in the framework for global data governance. Cooperation within each pillar occurs at multilateral, regional, plurilateral, or bilateral levels where there is sufficient trust and shared interests among the parties involved. Domestic requirements and international cooperation on cross-border data flows can be categorized into at least four pillars, each with a distinct but non-exclusive purpose: transfer mechanisms, legal and regulatory cooperation, technical standards and industrial cooperation, and international trade rules.

The challenging issue to the governance of global data is the difference in approaches taken by the governments. While some jurisdictions apply data protection rules equally to both foreign and domestic entities without any differentiation, most countries differentiate between them, especially for data related to national security. These jurisdictions may also label specific entities as either trusted or high-risk, with some even classifying all data as sensitive without

[155] Government of Japan, Ministry of Economy, Trade and Industry (METI), "G20 Ministerial Statement on Trade and Digital Economy", 9 June 2019.

the category of critical data. Legal and regulatory cooperation involves intergovernmental efforts to establish best practices and common normative principles, sometimes extending to the harmonization of domestic laws. The OECD, for instance, has created detailed privacy legislation guidelines that encourage its member countries to harmonize their domestic regulations, and these guidelines are referenced in some trade agreements.[156] Regulatory cooperation is also evolving within regional co-operations such as ASEAN, where legal alignment on data governance and privacy is being developed alongside internal data flow mechanisms.[157]

If legal, regulatory, and technical cooperation all work together and primarily builds the trust needed for openness, the role of trade rules is just to establish binding disciplines that protect this openness. Trade agreements which requires contracting parties to commit to non-discrimination in agreed-upon areas. At a multilateral level, many World Trade Organization (WTO) rules are pertinent to the digital economy, even though they were established before the internet's creation. Additionally, a WTO panel has also ruled that members must permit information transfers in sectors where they have market access or national treatment commitments.[158] Invoking privacy exceptions to these commitments would also be subject to specific conditions.[159]

The balance in Prime Minister Abe's speech and the duality of the Data Free Flow with Trust (DFFT) concept—where data flows where there is trust—are crucial to the Osaka Track. The idea of interoperability is also central, as it can foster trust across all pillars of the Osaka Track. However, the broader societal challenge extends beyond this: technical infrastructure is necessary to share data and ensure its use across different systems. Additionally, people need to be able to interpret the data and apply it in new contexts.[160] Despite these challenges, there are examples of international cooperation between countries still working to develop trust.

[156] Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data", 2013, referenced in United States-Mexico-Canada Agreement Article 19.8.
[157] Association of Southeast Asian Nations (ASEAN), "The 18th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN)", 2018.
[158] World Trade Organization, "DS413: China – Certain Measures Affecting Electronic Payment Services", 2012.
[159] The two-tier test established under GATT XX also applies to GATS general exceptions according to World Trade Organization, "DS285: United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services", 2005.
[160] Gasser, Urs, "Interoperability in the Digital Ecosystem", Berkman Klein Center for Internet & Society, Harvard University, Research Publication no. 2015-13, 2015.

Given the open nature of the internet and the global trading system, governments must also allow for alternative mechanisms (such as the certification of trusted businesses) when intergovernmental cooperation cannot provide an immediate solution.

Discussions with World Economic Forum stakeholders on achieving the Data Free Flow with Trust (DFFT) vision highlighted numerous forums, pillars, and levels of cooperation that shape global rules on data governance. Openness and interoperability for cross-border data flows depend on mechanisms and collaborations that foster trust. The architecture of the Osaka Track demonstrates various configurations for achieving free and trusted data flows, although there are opportunities for improvement as identified in the mapping process, which revealed significant gaps. These gaps need to be addressed by recommending the governments with proposed guidelines and co-operational policies.

The recommendations to fasten the growth of Osaka Track includes the developed economies, international organizations, and the business community should provide technical assistance and capacity-building tools to enable developing economies to adopt high-standard data governance policies and practices. This support is crucial to ensuring that the benefits of digitalization reach all citizens. Addressing data governance gaps is essential as they present challenges and restrict policy options, particularly if advanced economies question the treatment of data in developing countries. Transfer mechanisms should be designed to minimize compliance costs and complexity, ensuring that developing countries and micro, small, and medium enterprises (MSMEs) can fully participate in global trade.

Other recommendations include the Governments to implement robust privacy and security protections that does not restrict the flow of data but empower users to individually control their rights over personal information by giving consent or withdrawal of consent for each and every process and activity of data used, aligning with international guidelines and standards. Stakeholders have already highlighted the significance of frameworks such as the OECD Privacy Framework and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Transfer mechanisms in this matter as they play a crucial role in preventing de facto data localization which is considered to be a significant hinderance to the whole concept of Osaka Track and Data Free Flow with Trust. This paper presents several transfer mechanisms that enable a trusted flow of personal information to third countries, even in jurisdictions with differing levels of protection unlike the General Data Protection Regulation

of European Union which allows only to third countries with adequate data protection. Some regulations apply extraterritorially, ensuring that "data protection travels with the data." Therefore, governments must ensure the availability of multiple mechanisms and exceptions for non-discriminatory cross-border transfers of personal data under similar conditions.

Hence, the impact of cross border data flow is global, there is an urgent need to address the governance of the cross border data flow at the international level. Many international organisations have taken many initiatives but have failed to provide a comprehensive legal framework at the international level. The Data Free Flow with Trust is seemed to be a welcoming path to the Global Data Governance which strikes the balance between the free flow of data and economic prosperity and the protection of privacy and national security. Hence, governments must take part in the Osaka Track negotiations and come up with a binding legislative framework which the governments can incorporate into their domestic legislations.

Chapter 5: Findings and Conclusion

Having dealt with the concept of cross border data flow, the international and regional policies governing it, its relation with the International trade especially in the context of digital trade, its economic and social impact on India and the evolution of data policies of India, it is evident that the governance of cross border data flow needs attention both at the national and the international level. The framework of the global data governance should be the one that achieves a balance between allowing free flow of data considering its importance in the digital world and at the same time provide protection to the right of privacy of individuals. This is where a new rules or subordinate legislation at the national level and the concept of Data Free Flow with Trust (DFFT) as mentioned in the previous chapter will create wonders and sooner the countries co-operate, the better.

Part A: Key Findings

This Part will be a short summary of the key findings in this dissertation. So, throughout this dissertation, the first and key finding has been the lack of clarity in the legislative competence at the international level. Data is considered to be the 'new oil' as it holds immense potential and economic value to it. These economic and social value can be achieved only when it is allowed to flow across countries. Hence the international governance of the cross border data flow is very important. Even though the international organisations like the OECD has proposed privacy guidelines from time to time but it is considered as failure since many governments failed to adopt the same and implement in their domestic legislations. This led to the creation of various regional policies such as the European Union's General Data Protection Regulation (GDPR), APEC's Cross Border Privacy Rules, etc. which incorporates various approaches to the cross border data flow. Hence, there is no uniformity in the global data governance which hinders the economic prosperity of the value of data in the digital world. Until now, there is no any specific international framework or authority that addresses this issue. Efforts have been taken lately which was initiated by the Japan's Prime Minister in the year 2019 through a concept of 'Data Free Flow with Trust (DFFT)' which provides a promising path in achieving the balance. It is a concept that proposes the idea that data will flow where there is trust. Even though the concept slightly sounds like GDPR, it is not stringent enough like GDPR which imposes stringent restrictions on data flow and the word free flow

also doesn't mean that there will be no guidelines for protection. The core architecture of the DFFT is to propose necessary protection measures and mainly to bring co-operation among governments and propose binding and non-binding rules for the government to incorporate in their domestic legislation.

The next key area covered in this dissertation is the Digital Personal Data Protection Act, 2023 and its evolution that had key implications on cross border data flow in India. It is always the privacy protection laws and rules that mostly governs the cross border data flow in a country. After years of public debates and withdrawal of bills, the Digital Personal Data Protection Act, 2023 is the comprehensive legal framework that governs cross border data flow. Even though the Act brought significant frameworks for the data protection by establishing the Data Protection Board of India and providing obligations for Data fiduciaries and Significant data fiduciaries, it failed to address the issue of cross border data flow. One of the major drawbacks with respect to governance of data flow is the ambiguity surrounding the blacklisting of countries under the Act to which data transfers are strictly prohibited. With ambiguity surrounding it, many business entities are now hesitant to invest in India and have business connections and provide services as they will be forced to comply with the data localisation measures. This brings in an economic setback to the country both in the ways of investments in India and also through the restriction of data flow which brings in decreased volumes of goods in trade especially the digital trade. Hence the issue of blacklisting of counties needs to be addressed by a fresh set of rules or a subordinate legislation to the main Act which proposes the determined set of principles and grounds followed in blacklisting of countries. Developing countries like India should participate but not wait for international co-operation on the discussion of Data Free Flow with Trust and should clear the ambiguity in its own legislations that govern cross border data flow to increase its wealth and prosper economically. The new set of rules or subordinate legislation in addition to the guidelines on blacklisting, must also have the guidelines and procedures that the companies should follow in case of data breaches or certain incidents, etc.

The third key area covered is the data localisation measures and its impact on cross border data flow and its scope of protection on cybersecurity and privacy of individuals. Data localisation is a like a coin which has both heads and tail, it has both positive and negative impacts to a country. The positive impacts include bringing in new investments through the building of data servers and cloud servers and providing digital data services like the cloud

computing, etc. Hence it brings in a lot of economic opportunities through various business entities and through this a lot of employment and job opportunities are also created in the country resulting in economic proliferation. Other positive impacts include better governance of data by the government if the data is stored locally within the territory of the country. It helps in taking better actions against private entities or also help the criminal investigation by providing data when it is stored locally. It is also difficult to make a foreign entity liable under the local jurisdiction of a territory thus making it difficult if the data is allowed to transfer across the country. Primarily data localisation measures are laid on the grounds of cybersecurity and protection of right to privacy of individuals. Whereas the negative impacts which are often supported by the technical studies show that, in the context of cybersecurity, data localisation has no scope to do as it does not reduce the number of cyberattacks. Cyberattacks are basically dependent on the software used in the cybersecurity measures and not dependent on the location of data. Technical studies often show that data travels very fast across countries that it is not nearly possible to track down a data in a particular time. Both in the context of cybersecurity and protection of privacy, data localisation will only make it more vulnerable to cyberattacks and data breaches, as it makes the data stay in few domestic servers who may not even have the advanced cybersecurity technologies making it easier for the attack. In the context of economic impact, it is very evident that cross border data flow and digital trade contribute significantly to the GDP of a nation and that restrictions in the cross border data flow will definitely have an economic setback. Even though the data localisation brings in lot of economic opportunities, it does not apply to all countries and if the positive and negative impacts of the data localisation measures are weighed, it is very evident that the negative impacts are significantly higher than the positive impacts.

Above all, the important step to transform the framework of cross border data flow and protect the rights of privacy as well will undoubtedly be the introduction of a new set of rules or subordinate legislation to support the existing DPDP Act, 2023. A fresh sub-ordinate legislation can help solve the confusions that remain on the topics of blacklisting of countries, data localisation measures, guidelines for industries and entities, etc. The aspects to consider while framing such a sub-ordinate legislation includes non-discrimination principle, categorization of data to separate the critical personal data and impose only partial data localisation measure making only the critical personal data to be stored in India and making the other types of data to be flown freely outside the territory considering its economic value in the modern world.

Part B: Conclusion

India's cross border data flow framework is not perfect. But, the country is, in fact, has the potential to become one of the most effective regulators of cross border data flow and protectors of the privacy in the world. The reason for India being in such a great position is the implementation of the Digital Personal Data Protection Act, 2023 after nearly 4 years of struggle. The Act contains plethora of provisions giving priority in the field of the consent of individuals, obligations of data fiduciaries which have made things such as the privacy protection of individuals and data localisation clear. Yes, some doubts still remain in the areas of blacklisting but the cues can be taken from various sources. This includes European Union's privacy regulation which states that countries with non-adequate (not equivalent) measures are blacklisted. Even though a developing country like India should not impose very stringent measure like GDPR, concepts can be taken and amended to the circumstances of India. The solutions are right in front of the nation's eyes and it is only a matter of when the same is implemented.

As established earlier in the dissertation, cross border data flow is not a concept that involves only one country. Hence trying to confine it under a single nation will only bring problems to the country. Data Localisation has proved by several evidences that there are economic implications to a country if they implement these measures and they are not even fulfilling their aim and objective of cybersecurity and protecting the rights of the individuals. Hence countries instead of trying to govern the cross border data flow through data localisation measures, there should be a global governance of the same. This will be beneficial to the world GDP. Countries and International Organisations like the World Economic Forum are striving to create a middle path for the governance of data flow by the introduction of Data Free Flow with Trust. DFFT is seeming to be promising path for the future of cross border data flow governance as it helps in achieving the balance between the free flow and data protection. Hence governments should come in hand and participate in the discussion of the DFFT and make it a possible solution for the international framework for global data governance.

Therefore, the potential for things to go awry is very much present. There can be no denying that cross border data flow will not only bring economic benefits to a country but also other social benefits as well. Every business entity in the modern digitalised world are relying

heavily on the data transfer. So, regulations both at the national and international level are the only way in which social, moral and ethical responsibilities can be made essential. These regulations must be robust enough to strike the balance between economic benefits of data flow and protecting privacy and cybersecurity. The need for this balance while framing laws must be the biggest takeaway from this dissertation and the sooner a fresh set of rules or subordinate legislation to the Digital Personal Data Protection Act, 2023 is brought for governance of data flow, the better it will be for the organic growth of the digital trade, combined with user satisfaction.

Bibliography and References

Statues and Legislations

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981
- General Data Protection Regulation, 2018
- GATS 1994: General Agreement on Trade and Services, 1994
- Cross Border Privacy Rules, 2011
- Indian Telegraph Act, 1885
- Public Records Act, 1993
- Information Technology Act, 2000
- Information Technology *(Amendment)* Act, 2008
- Information Technology *(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)* Rules, 2011
- Personal Data Protection Bill, 2019
- Data Protection Bill, 2021
- The Digital Personal Data Protection Bill, 2022
- The Digital Personal Data Protection Act, 2023

Books

- Svetlana Yakovleva, *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law* (2024)
- Bryan Mercurio and Ronald Yu, *Regulating Cross Border Data Flows: Issues, Challenges and Impact* (Nov 2022)
- Mira Burri, *Big Data and Global Trade Law* (July 2021)
- Vanya Rakesh, *Privacy Symposium* (2022)

Journal Articles

- Qing Chang, Lin William Cong, Liyong Wang, and Longtian Zhang, *Production, Trade, and Cross-Border Data Flows*, NBER Working Paper No. 31416 (June 2023)

- Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?* World Trade Review (Forthcoming, 2019) (Pre-edited draft) NUS Centre for International Law Research Paper No. 19/11 (2019)
- Julian Rotenberg, *Privacy Before Trade: Assessing the WTO-Consistency of Privacy Privacy Before Trade: Assessing the WTO-Consistency of Privacy Based Cross-Border Data Flow Restrictions,* University of Miami International and Comparative Law Review, Volume 28 Issue 1 (Fall 2020)
- Casalini, F. and J. López González, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers, No. 220, OECD Publishing, Paris (2019)
- Neha Mishra, *Data localization laws in a digital world: Data protection or data protectionism?* The Public Sphere, NUS Centre for International Law Research Paper No. 19/05 (2016)
- Rajat Kathuria, Mansi Kedia, Gangesh Varma and Kaushambi Bagchi, *Economic Implications of Cross Border Data Flow*, ICRIER Reports, (Nov 2019)
- Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, GLOBAL ECONOMY & DEVELOPMENT WORKING PAPER 113 (March 2018)
- Evan A. Feigenbaum and Michael R. Nelson, *Data Governance, Asian Alternatives How India and Korea Are Creating New Models and Policies,* Carnegie Endowment for International Peace (2022)
- UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, Information Economy Report (2016)
- Macmillan Keck, *The role of cross-border data flows in the digital economy*, UNCDF Policy Accelerator (July 2022)
- W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'l L.J. 485 (2020)
- Smriti Parsheera and Prateek Jha, *Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?,* Carnegie India Working Paper (Nov 2020)
- Bacchus, James. "Cross-Border Data Flows." *The Digital Decide: How to Agree on WTO Rules for Digital Trade*, Centre for International Governance Innovation, (2021)
- Burman, Anirudh, and Upasana Sharma. "History of Data Localization." *How Would Data Localization Benefit India?*, Carnegie Endowment for International Peace, pp. 3–6. *JSTOR* (2021)

- Si Chen, *Research on Data Sovereignty Rules in Cross-Border Data Flow and Chinese Solution*, 18 US-CHINA L. REV. 261 (2021).
- Xia Han, *Paradigm Shift of European Union (EU) in Cross-Border Data Flow Supervision - From the Perspective of Digital Services Legislation*, 13 J. WTO & CHINA 69 (2023).
- Raj Shekhar & Aman Yuvraj Choudhary, *Data Localisation and Cross-Border Flow of Data: Balancing the Incongruent Dimension of Barriers, Safeguards and "Free Flow of Data"*, 2022 RGNUL FIN. & MERCANTILE L. REV. 19 (2022).
- Dan Jerker B. Svantesson, *The Regulation of Cross-Border Data Flows*, 1 INT'l DATA PRIV. L. 180 (2011).

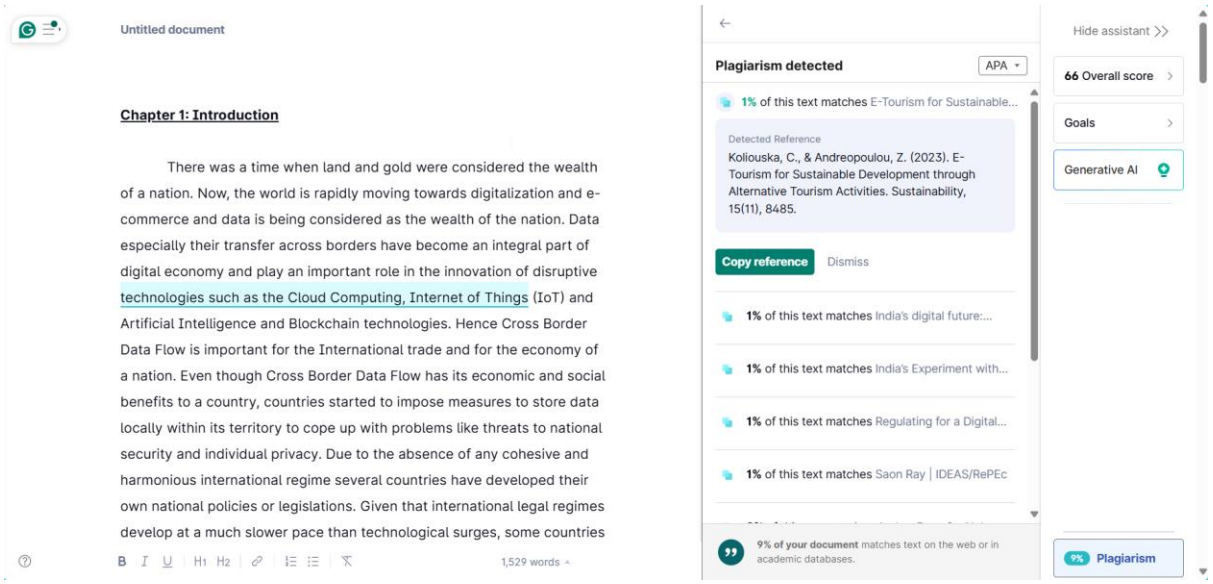
Web Sources

- Tanguy Van Overstraeten, *Cross-border data flows: A necessary part of global trade*, Digital Economy, Trade & External Affairs (2021) https://www.amchameu.eu/blog/cross-border-data-flows-necessary-part-global-trade (last visited June 22, 2024)
- Shruti Dvivedi Sodhi, Bansari Samant and Tushar Sinha, *The Journey of India's Data Protection Jurisprudence*, Khaitan Legal Associates (2022) https://www.lexology.com/library/detail.aspx?g=57720842-f709-4dd4-947b-44c3c6e4ed10 (last visited June 22, 2024)
- Patenge Chathrapathi, *Evolution of Data Protection in India; Detailed Analysis*, Legal Services India, (2023) https://www.legalserviceindia.com/legal/article-14487-evolution-of-data-protection-in-india-detailed-analysis.html#google_vignette (last visited June 22, 2024)
- Alan Sunny, *Data Privacy Regime in India: Its Genesis and Evolution*, MEDIANAMA (2022) https://www.medianama.com/2022/12/223-genesis-evolution-india-data-protection-regime-views/ (last visited June 22, 2024)
- Aidan Arasasingham and Matthew P. Goodman, *Operationalizing Data Free Flow with Trust (DFFT)*, Centre for Strategic and International Studies (CSIS), (2023) https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft (last visited June 22, 2024)

- Antony Cook, *Cross-Border Data Flows – Powering Innovation & Economic Growth*, LinkedIn, (2018) https://www.linkedin.com/pulse/cross-border-data-flows-powering-innovation-economic-growth-cook-1d/ (last visited June 22, 2024)
- Geoffrey Manne and Mikolaj Baeczentewicz, *Keeping data flowing is in India's interest*, TOI (2023) https://timesofindia.indiatimes.com/blogs/voices/keeping-data-flowing-is-in-indias-interest/ (last visited June 22, 2024)
- Shashank Reddy, INDIA'S APPROACH TO CROSS-BORDER DATA FLOWS, Goethe-Institut (2023) https://www.goethe.de/ins/in/de/kul/fmd/afu/25298606.html (last visited June 22, 2024)
- GV Anand Bhushan and Swasti Gupta, *India's digital future: Navigating cross-border data flows in the age of the fourth Industrial revolution*, TOI (2023) https://timesofindia.indiatimes.com/blogs/voices/the-digital-personal-data-protection-bill-2022-panacea-or-pandoras-box/ (last visited June 22, 2024)

PLAGIARISM REPORTS

Chapter 1 - 9%



Untitled document

Chapter 1: Introduction

There was a time when land and gold were considered the wealth of a nation. Now, the world is rapidly moving towards digitalization and e-commerce and data is being considered as the wealth of the nation. Data especially their transfer across borders have become an integral part of digital economy and play an important role in the innovation of disruptive technologies such as the Cloud Computing, Internet of Things (IoT) and Artificial Intelligence and Blockchain technologies. Hence Cross Border Data Flow is important for the International trade and for the economy of a nation. Even though Cross Border Data Flow has its economic and social benefits to a country, countries started to impose measures to store data locally within its territory to cope up with problems like threats to national security and individual privacy. Due to the absence of any cohesive and harmonious international regime several countries have developed their own national policies or legislations. Given that international legal regimes develop at a much slower pace than technological surges, some countries

1,529 words

Plagiarism detected

APA

1% of this text matches E-Tourism for Sustainable...

Detected Reference

Koliouska, C., & Andreopoulou, Z. (2023). E-Tourism for Sustainable Development through Alternative Tourism Activities. Sustainability, 15(11), 8485.

Copy reference Dismiss

1% of this text matches India's digital future:...

1% of this text matches India's Experiment with...

1% of this text matches Regulating for a Digital...

1% of this text matches Saon Ray | IDEAS/RePEc

9% of your document matches text on the web or in academic databases.

Hide assistant

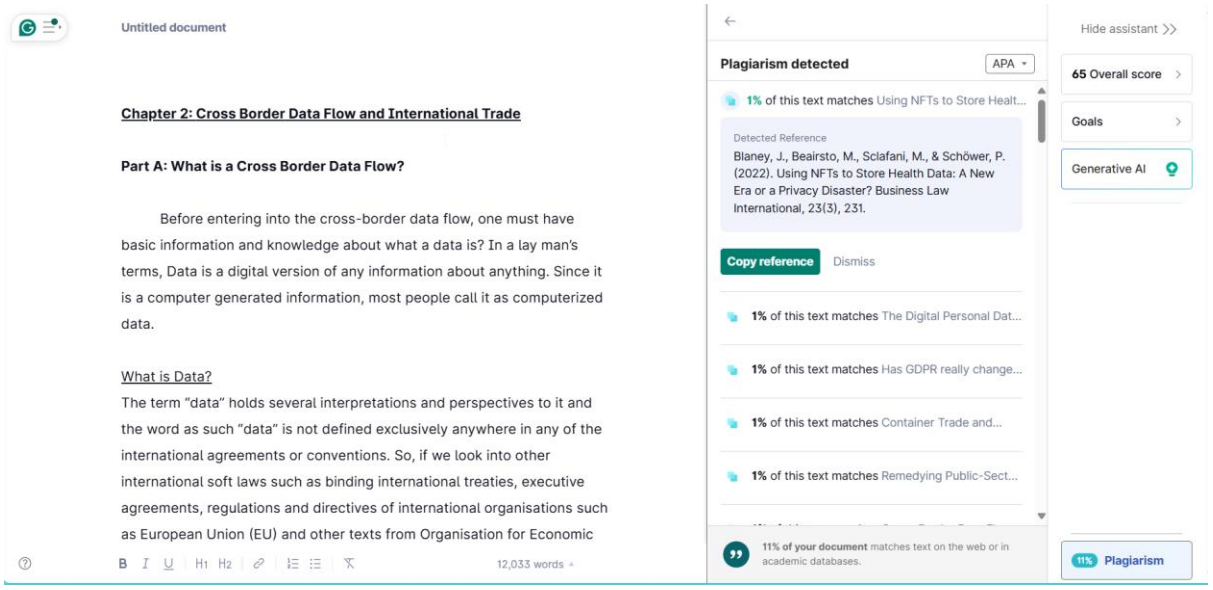
66 Overall score

Goals

Generative AI

9% Plagiarism

Chapter 2 - 11%



Untitled document

Chapter 2: Cross Border Data Flow and International Trade

Part A: What is a Cross Border Data Flow?

Before entering into the cross-border data flow, one must have basic information and knowledge about what a data is? In a lay man's terms, Data is a digital version of any information about anything. Since it is a computer generated information, most people call it as computerized data.

What is Data?

The term "data" holds several interpretations and perspectives to it and the word as such "data" is not defined exclusively anywhere in any of the international agreements or conventions. So, if we look into other international soft laws such as binding international treaties, executive agreements, regulations and directives of international organisations such as European Union (EU) and other texts from Organisation for Economic

12,033 words

Plagiarism detected

APA

1% of this text matches Using NFTs to Store Healt...

Detected Reference

Blaney, J., Beairsto, M., Sclafani, M., & Schöwer, P. (2022). Using NFTs to Store Health Data: A New Era or a Privacy Disaster? Business Law International, 23(3), 231.

Copy reference Dismiss

1% of this text matches The Digital Personal Dat...

1% of this text matches Has GDPR really change...

1% of this text matches Container Trade and...

1% of this text matches Remedying Public-Sect...

11% of your document matches text on the web or in academic databases.

Hide assistant

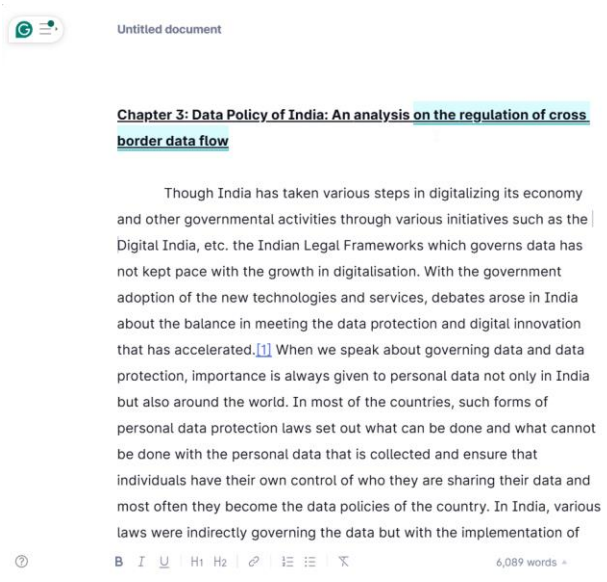
65 Overall score

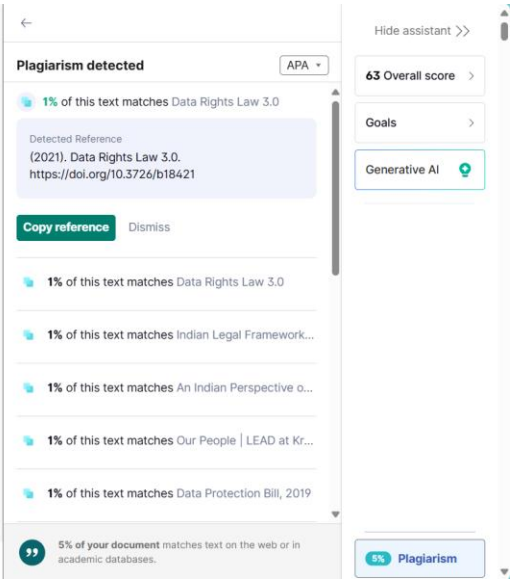
Goals

Generative AI

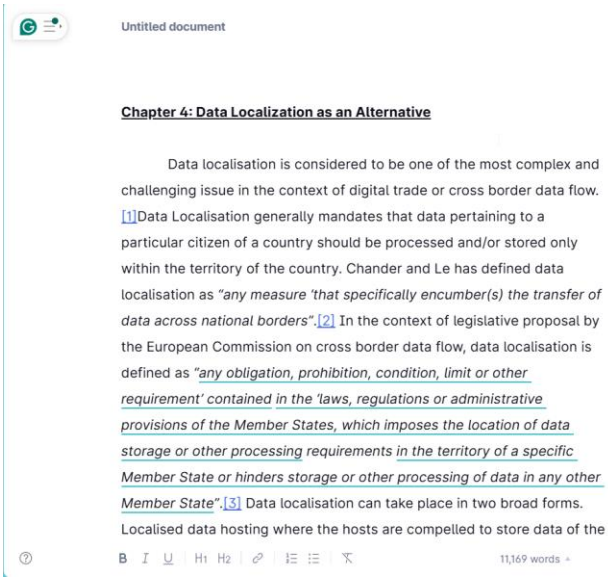
11% Plagiarism

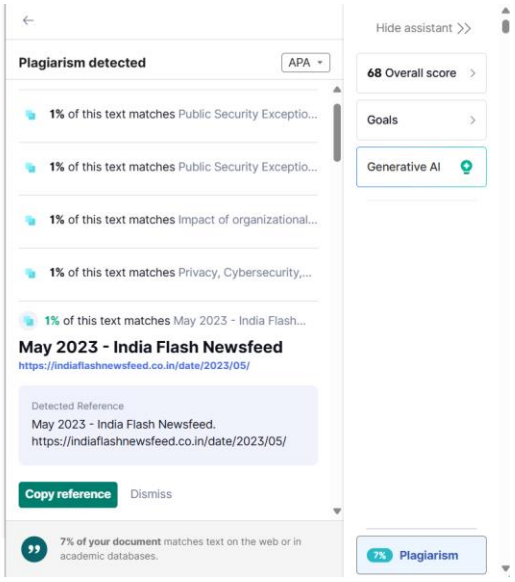
Chapter 3 - 5%



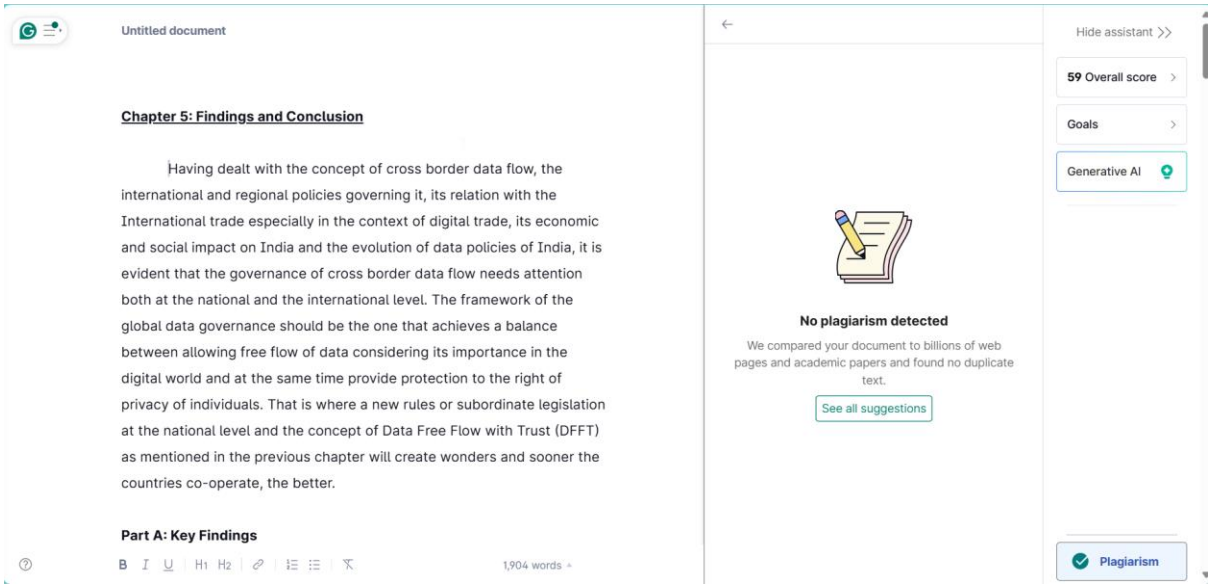


Chapter 4 - 7%





Chapter 5 - 0%


Untitled document
Chapter 5: Findings and Conclusion
Having dealt with the concept of cross border data flow, the international and regional policies governing it, its relation with the International trade especially in the context of digital trade, its economic and social impact on India and the evolution of data policies of India, it is evident that the governance of cross border data flow needs attention both at the national and the international level. The framework of the global data governance should be the one that achieves a balance between allowing free flow of data considering its importance in the digital world and at the same time provide protection to the right of privacy of individuals. That is where a new rules or subordinate legislation at the national level and the concept of Data Free Flow with Trust (DFFT) as mentioned in the previous chapter will create wonders and sooner the countries co-operate, the better.
Part A: Key Findings
1,904 words
Hide assistant
59 Overall score
Goals
Generative AI
No plagiarism detected
We compared your document to billions of web pages and academic papers and found no duplicate text.
See all suggestions
Plagiarism