Data Protection Standards for Transborder Data Transfer: Approaches and Way Forward

Satya Vrat Pandey*

Abstract: In the age of fast technological improvements and the virtual revolution, the problem of privacy and information safety has grown to be paramount. Privacy and information safety rules are to strike a sensitive stability between permitting innovation and safeguarding people's essential rights. These rules set up recommendations and frameworks that govern the collection, use, storage, and sharing of private information through entities which include agencies, governments, and carrier providers. Key additives of information safety rules consist of the requirement for express consent from people earlier than processing their information, making sure the statistics amassed are constrained to the reason for which it turned into obtained, and ensuring information accuracy and security. Moreover, those rules make bigger past country-wide borders, impacting agencies working internationally. Further, continuous updates and worldwide cooperation may be vital in addressing rising demanding situations and making sure that those rules stay powerful in a swiftly evolving technological panorama.

Keywords: *Cross-border data, Privacy, Flow, India, International, Digital Economy and stakeholders.*

1. Introduction

The transfer of cross-border data is the most vital aspect of the global economy, from enabling innovation, value, and wealth to carrying information cross-border data transfer plays a very crucial role. When the cross-border transfer of data takes place, it becomes even more crucial for stakeholders to ensure the free flow of data, to deliver more to more people, and to generate newer opportunities and benefits for the people and the planet. Global trade and the transfer of cross-border data are interconnected. The transfer of data across borders is a major facet that assists in promoting the exponential growth of international trade.

In the present global digital world, internet-based advertisement and retailing, electronic payment systems, and on-demand computing have become essential elements of the overall business industry, in fact in the present scenario it is impossible to imagine international trade that does not require data transfer. Several countries have come up with various approaches, regulations, and mechanisms to regulate the data flow across borders, effectively tackle

* Fourth Year, BA. LL. B, Faculty of Law, Integral University, Lucknow

national security, intellectual property, and privacy, or protect domestic jobs. However, some countries even put certain restrictions on the flow of data across borders, even if the intention behind such restrictions is mala-fide, it can lead to challenges such as data fragmentation and could weaken the global trade flow. Presently, many countries have been regulating cross-border utilizing several models, including the Asia-Pacific Economic Cooperation (APEC), the European Union's General Data Protection Regulations (GDPR), and the Privacy Framework of the US. Despite these frameworks, a need for a more stringent legislative framework is necessary to regulate cross-border data transfers, as many countries still lack laws that effectively safeguard personal data and a lack of consistency is evident between different frameworks.

As the global data flow is increasing day by day, a well-formulated legal framework could ensure the seamless transfer of cross-border data and prevent its misuse in terms of data breaches, national security, and personal data privacy concerns. Such a framework is also essential for the economic growth of the country. Such as in the case of India, although the Union government has come up with legislation like the Digital Personal Data Protection Bill, 2022, hereafter DPDP, still such legislation has some lacunas Clause 17 of the DPDP Bill, 2022[1] fails to address whether the Union government allows the transfer of data with certain restrictions to other country or completely bans all cross-border data transfers until the government "White List" that country.

This paper highlights the importance of implementing a sensible strategy for controlling international data transfer for India to ensure a seamless flow of cross-border data. The paper in its second portion advances towards promoting the collective efforts of stakeholders to create a culture of data-free flow with trust. It also addresses the methods to maintain confidentiality and safeguard personal data and contemporary and modern consent processes for data transfer outside of India, the second last portion of the essay deals with the role and effect of cross-border data transfer on the Indian Economy and lastly, the essay suggests approaches, that could help India in ensuring a seamless transfer of cross-border data.

2. A Sensible Strategy for Controlling International Data Transfer

India needs to regulate cross-border transfers in an exhaustive and advanced manner that equalizes the objectives of the nation's safety, creativity, and development in the economy. Strong laws regarding data protection must be put into place. Recently, the bill on the protection of personal data passed in India; is currently pending legislative approval. By providing measures for cross-border data transfers, this Act intends to create an outline for the security of personally identifiable information. Legislation should strike a compromise between protecting

[1] Digital Personal Data Protection Bill 2022, cl 17

individual privacy rights and facilitating data transfers for legal purposes.[2] Cross-border transmissions of data can benefit from a risk-based strategy, which can assist in concentrating laws and regulations on vulnerable operations.

The amount of inspection and requirements placed on data transfers can be determined by evaluating the possible impact of confidentiality and national security, with greater controls being applied to receptive data and important industries.

Creating an impartial regulatory body with adequate funding to monitor international data flows is crucial. This body should have the capacity to investigate infractions, issue sanctions, and provide organizations advice. User permission is one of the key components of both data localization and cross-border data transfer. Consent is essential to the collection, processing, storage, and sending of data.

Businesses and corporate organizations must legally make sure that the data subjects are informed, and informed permission is acquired before data collection and transmission. Such permission is frequently contractual and revocable at the data subject's discretion. Gaining the agreement of the data subject is a crucial need for cross-border data transmission given the absence of an information protection regime. To promote trust and conformity, enforcement measures should be reasonable, identical, and open. There are three data models: one based on publicly available information transfers and processing, another with conditional transfer and processing, and a third one based on constrained data transfers and processing.[3] When drafting their laws for the national handling of sensitive information as well as the cross-border transfer of personally identifiable information, many other countries now use these three data models as a reference.

India may think about implementing a middle approach between the open model and the conditional model, one that is neither too strict nor too lax, to preserve an equilibrium between the development of a nation and data privacy, among all three approaches for regulating cross-border data transfers, namely the open model, the conditional model, and the control model. It is important to work to advance global commerce while preserving national security and the rights of data subjects, as well as without impeding technological advancements or economic expansion.

[2] 'Enabling Accountable Data Transfers from India to the United States under India's Proposed Personal Data Protection Bill' (*Information Policy Centre*, 2020) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-dsci_report_on_enabling_accountable_data_transfers_from_india_to_the_united_states_under_indias_proposed_pdpb_8_september_2020_.pdf> accessed 13 July 2023

[3] Mihail Danov, 'Data Analysis: Important Issues to Be Considered in a Cross-Border Context' (*Semantic Scholar*, 2021) <https://www.semanticscholar.org/paper/Data-Analysis%3A-Important-Issues-to-be-Considered-in-Danov/061b18d3dff36782e0091569f8c14438e4811a2e> accessed 13 July 2023

3. Collective Efforts of Stakeholders to Create a Culture of "Data-Free Flow with Trust"

The world's data policy environment is still complicated, and it is expected to get even more so as more nations embrace the localization of information policies. To make matters worse, these policies are getting more onerous. Data Free Flow with Trust must thus be realized today to properly minimize the costs and hazards brought on by international segmentation; otherwise, it is likely to remain a concept that will never come to pass. A Partnership between the government and industry is required to realize Data Free Flow with Trust by conquering complicated political fragmentation by creating and increasing trust. Public-private partnerships that knowledge and experience from around the world should lead to the development of a reliable and efficient mechanism to promote more interoperability as well as practical tools for companies to reduce the risk and expense of transferring data across borders. The dialogue among governments and other stakeholders as they develop new cross-border data governance models may benefit greatly from this contribution to the discussion. Law authority demands access to information housed in another country's jurisdiction are governed by ineffective procedures and outmoded legal agreements, which should be revised by the relevant countries. National law administration organizations must have confidence that they may access local data, related to lawful law enforcement investigations, kept in other countries if we are to develop a broadly disseminated open exchange of data with a trust framework. To enable Internet suppliers to stop data flows involving the illegitimate use and dissemination of unauthorized information, nations should provide regulatory and bureaucratic structures with the corresponding checks and balances.[4] Given that certain data flows are legitimately unlawful, it is crucial to understand that some information flows should be regarded equally when discussing the idea of data circulating freely with trust.

Leading digital economies should share Australia's understanding that site banning is a useful instrument for enforcing intellectual property laws, as do Singapore, the United Kingdom, and a large number of other nations. Nations should promote encryption's function in safeguarding communication of information and digital technology, not weaken it. Data must be sent with trust, and cryptography is an essential innovation that people and organizations use to protect data secrecy. Any attempt of an authority to compromise cryptography diminishes the general safety of constitutional individuals and organizations, makes it harder for enterprises from nations where cryptography is weak to succeed on the international stage, and halts the progress of safeguarding data. To do this, India may run engagement activities with groups of stakeholders that might aid with comprehending their goals and potential difficulties with international data transmissions. While addressing the security of the transferred

[4] Vikram Jeet Singh, *et. al*, 'Privacy Week Series: Analyzing Cross-Border Data Transfer Mechanisms - Privacy Protection - India' (*Mondaq*, 23 February 2023) <https://www.mondaq.com/india/privacy-protection/1276438/privacy-week-series-analyzing-cross-border-data-transfer-mechanisms#:~:text=It%20offers%20a%20> accessed 13 July 2023

data, this strategy will boost the opportunity of the various stakeholders and enable a larger, broader atmosphere for cross-border data transfers amongst stakeholders.

4. A Contemporary and Modern Consent Process for Data Transfer Outside of India

In the current world, confidentiality and safeguarding of personal data have been elevated to one of the most crucial facets of someone's life. A comprehensive piece of law on the subject is required to regulate such a critical topic. Every law regulating the confidentiality of information is built on the principle of consent. Before utilizing or acquiring someone's personal information, it is a widely accepted practice to get that person's consent, and the DPDP Bill, 2020[5] has included this practice. Only legitimate uses and with the information subject's express or implied permission are permitted for the processing of identifiable information. With its recent arrival, the idea of deemed Consent aids in reducing the need for further permission. Personal information may be transferred outside of India by the data fiduciary to nations that it has been authorized to do so by the interference of the government. Of course, this would depend on the data being adequately protected, as well as on equality, straightforwardness, and equality across nations—all characteristics that any contemporary legislation should have. Instead of adopting the customary way of obtaining approval from the data subjects, the Rules shall give a stronger approach to the consent process in cases of cross-border data transfer. Because there is a low level of digital literacy in India, it can be difficult to obtain the actual consent of those persons who are unaware of the conditions, objectives, and types of data involving it being requested. Rules must define what is meant by explicit consent, and every time data is transmitted outside of India, further, separate consent is required. Consent applications should be focused and specific to minimize ambiguity or wide phrasing. The breadth of a person's consent should be up to them to decide and they ought to have the capacity to comprehend exactly what it entails. Contracts, intra-group conventions, and validity determinations are practical methods for enabling the transfer of data across borders that are in line with the principles enshrined in other contemporary privacy legislation.[6] Individuals may get confused and mistakenly believe that such transfers are inherently hazardous or improper if every cross-border transfer of sensitive data requires their approval.

Transfers are crucial to the supply of a vast array of goods and services for customers in the contemporary global digital economy. Individuals may be discouraged from utilizing the entire range of offered offerings and amenities, regardless of whether they would gain something from doing so, if consent is required for each exchange of sensitive data that may, in any case, be made secure through a variety of different transfer channels. Because an

[5] Digital Personal Data Protection Bill 2022, cl 17

[6] 'India: Best Practices for Cross-Border Data Transfers' (*Data Guidance*, 27 October 2022) <https://www.dataguidance.com/opinion/india-best-practices-cross-border-data-transfers> accessed 13 July 2023

entity may not have a connection with or contact information for the person whose identification data is being transmitted, it may occasionally be impractical to get consent regarding the exchange of confidential information. An institution may be required by law to reveal sensitive data, such as monetary data, even when it has no direct contact with the person in question while providing services connected to preventing financial misconduct.

5. Current Policy Procedures and Resources

According to a report by the Organisation for Economic Co-operation and Development (OECD), various initiatives, agreements, and processes tend to encourage seamless cross-border data transfer.[7] Several regulations and policies have been developed by the countries to unilaterally administer the transfer of cross-border data and to strengthen international relations. Additionally, initiatives adopted by global forums, have aided in promoting cooperation.

This includes:

a) Initiatives by G-20 and G-7 countries;

b) Analysis as well as research, setting specific standards and initiatives that are utilized to promote dialogue and cooperation in international institutions;

c) Various preferential permanent trade agreements with territorial organizations.

6. Policy process for cross-border data flows

6.1. Unilateral regulations and policies

The domiciliary methods mentioned below, promote the flow of cross-border data of definite types of data to other nations under certain conditions:[8]

Open Safeguard Method: According to this method, the cross-border data transfer could be initiated without any prerequisite criteria and this method is based primarily on the idea to protect public policy objectives.

[7] 'Cross-Border Data Flows' (*OECD*, 12 October 2022) <https://www.oecd.org/publications/cross-border-data-flows-5031dd97-en.htm> accessed 13 July 2023

[8] Francesca Casalini, *et. al*, 'Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers' (*Research Gate*, 2021) <https://www.researchgate.net/publication/356435860_Mapping_Commonalities_in_Regulatory_Approaches_To_Cross-Border_Data_Transfers> accessed 13 July 2023

Pre-authorized Method: In compliance with this method, cross-border data transfer is mostly initiated based on certain pre-conditioned rules and regulations. It involves the ex-ante trusted data transfer within the public sector such as; domestic certification programs, and preapproval of corporations' binding corporate laws.

6.2. Intergovernmental level processes

Multilateral initiatives: Analysis and research, standard-setting initiatives that are utilized to promote dialogue and cooperation in multilateral institutions like the UN, OECD, and World Trade Organization.

Regional arrangements: Various preferential permanent trade agreements with territorial organizations like ASEAN, APEC, and the European Union.

Preferential trade agreements: The are several treaties that promote trade barriers and define a certain set of rules for global trade and commerce between two countries or among a group of specific countries like the EU-UK Trade and Cooperation Agreement, UK, Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], Singapore Digital Economy Agreement.

In 2022, at the G7 summit held in Germany, DFFT was considered one of the six major points of discussion by digital ministers from member countries and adopted a G7 Action Plan Promoting Data Free Flow with Trust.

Such as:

a) Protecting the evidence base for DFFT;

b) Creating an environment to build on commonalities to promote future interoperability;

c) Sustained cooperation among the stakeholders;

d) Promoting a seamless cross-border transfer of data by inculcating DFFT in the global digital trade; and

e) Equal participation of all the countries in promoting and safeguarding data and sharing a common idea about the prospects for the transfer of data across borders.[9]

[9] 'Ministerial Declaration: G7 Digital Ministers Meeting' (2022) <https://www.bundesregierung.de/resource/blob/998440/2038510/e8ce1d2f3b08477eeb2933bf2f14424a/2022-05-11-g7-ministerial-declaration-digital-ministers-meeting-en-data.pdf> accessed 13 July 2023

In 2022, at the G20 summit held in Indonesia, the G20 Digital Economy Ministers' meeting expressed its concerns about promoting elements of convergence between existing regulatory approaches, complementarities, commonalities, and instruments enabling data to flow with trust, to foster future interoperability.[10]

7. Cross-border Data Flow and Indian Digital Economy

This section of the essay critically analyses the relationship between cross-data border flow and the Indian digital economy. As India's digital economy is on the rise, it is no secret that data is one of the most vital forces that contribute immensely to this growth. Analyzing the earlier growth of India's digital economy, it is evident that the value of the digital sector of India is projected to cross $1 trillion by 2025[11], and from the growth trends, it could be denoted that the Fourth Industrial Revolution is underway. As the digital spectrum of the Indian economy is growing daily, issues related to data protection and privacy breaches are also on the rise. When it comes to the digital economy, Cross border data transfer is one of the most important facets of the digital economy, which involves the flow of data from one nation to another. However, the problem arises as privacy laws and data protection laws are becoming more and more fragmented around the world. This gives rise to certain restrictions in cross-border data flow and puts global trade and economic and social activities at risk. In the ongoing policy debates it seems that the effect of cross-border data flow on the Indian economy has been underestimated. A study conducted by the Indian Council for Research on International Economic Relations revealed that a minimal decrease of 1% in the flow of cross-border data could result in a loss of trade of nearly $696.71 million for India. This study highlights the importance of the unrestricted flow of data for the economic growth of India and any barriers to the flow of data could pose severe challenges to India's trade and overall prosperity.[12]

Concerning the efficient flow of cross-border data, the government has raised major concerns and has advised law enforcement agencies to carefully handle the data, to prevent breaches of data and minimize the risks of social and economic imbalance. While the address of such issues is of utmost importance, taking a whitelist approach as seen in the earlier cases has ultimately burdened the cross-border data flow. However, to ensure a smooth transfer of cross-border data, data privacy laws implemented by the government must be followed religiously to ensure a balance

[10] 'G20 Digital Economy' (2022) <https://www.g20.org/wp-content/uploads/2022/10/G20-DEMM-Chairs-Summary.pdf> accessed 13 July 2023

[11] GV Anand Bhushan and Swasti Gupta, 'India's Digital Future: Navigating Cross-Border Data Flows in the Age of the Fourth Industrial Revolution' (*The Times of India*, 24 April 2023) <https://timesofindia.indiatimes.com/blogs/voices/the-digital-personal-data-protection-bill-2022-panacea-or-pandoras-box/> accessed 15 July 2023

[12] 'How Preferential Trade Agreements Affect the U.S. Economy' (*CBO*, 2016) <https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/51924-tradeagreements.pdf> accessed 15 July 2023

between law enforcement and the protection of the privacy rights of the citizens. The lack of effective mechanisms in the USA for regulating data protection and privacy legislation has led to stricter federal and state laws, which has aroused a difficult situation for businesses to adhere to and fulfill all the requirements of the legislation. However, on the other hand, the General Data Protection Regulation (GDPR)[13] adopted by Europe proved effective in protecting personal data and ensuring cross-border data flow. However, in the case of Asia, the privacy and data protection laws differ considerably, from China's effort to adopt cyber-sovereignty by critically administering the transfer of cross-border data to Japan offering comprehensive protection. Hence, the approach of laissez-faire adopted by the US, the concept of individual rights adopted by the European Union, and the focus on national interests displayed by China, are subject to considerable differences.

8. Approaches that could help India in ensuring seamless cross-border data transfer.

Various approaches such as legislation on data transfer, certification of industries, and making stakeholders aware of their duties towards handling data cautiously, have been adopted by the countries to ensure smooth cross-border data flow. It could prove helpful for India, to learn from the experiences of these nations while developing its course of action towards administering cross-border data transfer. Under the Digital Personal Data Protection Act of 2022, the union government will form a list of countries known as the White List and countries falling under that list will be notified for cross-border data transfers. Although, there have been no specific criteria for selecting the countries that will be on the list are yet to be known. It is pertinent from the above facts that the approach of the DPDP Bill, 2022[14] is quite unclear and it will require India to enter lethargic negotiations with numerous countries to successfully whitelist them thereby de-facto blacklisting the countries with unsuccessful or pending negotiations. Another lacuna in the DPDP Bill 2022[15], that could pose a major issue for India is Clause 17 of the DPDP Bill, this clause fails to clarify whether the Union government prohibits the transfer of data to another country or completely bans all cross-border data transfers until the government white list that country.

For India, to resolve the issues of cross-border data transfer and the unclarity involved in mentioning the countries in the White List, it must adopt the Black List Approach, which involves the free flow of data until a country is not blacklisted or bared specifically. Adopting this approach will allow an uninterrupted flow of data without any market or trade disruptions. Moreover, India can consider the following statutory provisions to ensure the seamless transfer of cross-border data[16]:

[13] General Data Protection Regulation 2016
[14] Digital Personal Data Protection Bill 2022, cl 17
[15] *Ibid*
[16] How Preferential Trade Agreements Affect the U.S. Economy (n 12)

Firstly, the Indian government must reframe the legislation which should define the word adequate in terms of the protection of data and standards of privacy. This legislation must also establish clear standards to evaluate other countries based on their data protection standards. Secondly, the legislation framed by the Indian government must grant permission to multinational companies to use Business Corporate Rules (BCRs) as an instrument of data transfer. Moreover, multinational companies adopt BCR rules as these rules provide sufficient protection against data breaches across several countries and allow businesses in India to ensure seamless data transfer within their international domains.

Lastly, the model contractual clauses could be used as another adequate mechanism for data transfer. These clauses ensure the transfer of data on a contractual basis and are approved and standardized by regulatory authorities as well. These statutory provisions would help businesses in India to transfer data to other countries and maintain privacy standards and proper data protection.

9. Conclusion

In conclusion, information safety for switches in India is a crucial problem that calls for cautious attention and powerful measures. The suggestion strategies mentioned in this challenge provide capacity answers to deal with the demanding situations related to information transfers, at the same time as making sure the privacy and safety of private statistics. The first proposed method, the enactment of complete information safety legal guidelines, is critical to setting up a sturdy criminal framework that governs information transfers. Such legal guidelines need to comprise concepts of transparency, accountability, and consumer consent and need to offer people enforceable rights and remedies. Additionally, the established order of an impartial regulatory authority can ensure powerful oversight and enforcement of those legal guidelines. The 2nd proposed method, the adoption of worldwide information switch mechanisms, acknowledges the significance of world information flows for monetary boom and innovation.

Implementing mechanisms consisting of general contractual clauses, binding company rules, or acquiring adequacy selections from the European Union can facilitate lawful and stable cross-border information transfers. However, it's essential to make sure that those mechanisms are frequently reviewed and up to date to hold tempo with technological improvements and evolving privacy concerns. The subsequent steps in addressing information safety for switches in India require a collaborative attempt among the government, enterprise stakeholders, and civil society. It is essential to foster recognition and schooling approximately information safety rights and great practices amongst people and organizations. Additionally, carrying out worldwide discussions and negotiations on information safety requirements can assist in aligning India's guidelines with worldwide norms, selling harmonized

information flows. Furthermore, investing in technological answers consisting of encryption, anonymization, and stable information garages can decorate the safety of transferred information. The improvement of privateness- improving technology and the advertising of privateness via way of means of layout concepts can considerably contribute to safeguarding private statistics at some stage in transfers. India is an ongoing method that necessitates a complete method encompassing criminal, technological, and collaborative efforts. By enforcing the proposed strategies and taking the following steps, India can set up a robust information safety framework that safeguards privacy rights, fosters trust, and promotes accountable information coping with practices in an increasing number of interconnected worlds.