ILE LEX SPECULUM

VOLUME I AND ISSUE I OF 2023

APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION STANDARDS FOR TRANSBORDER DATA TRANSFER: APPROACHES AND WAY FORWARD

AUTHOR – SATYA VRAT PANDEY, STUDENT AT INTEGRAL UNIVERSITY, LUCKNOW

Best Citation - SATYA VRAT PANDEY, DATA PROTECTION STANDARDS FOR TRANSBORDER DATA TRANSFER: APPROACHES AND WAY FORWARD, *ILE LEX SPECULUM (ILE LS)*, 1 (1) of 2023, Pg. 38-44, APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2.

Abstract

In the age of fast technological improvements and the virtual revolution, the problem of privateness and information safety has grown to be paramount. As people and companies embody the virtual panorama, the extent of private information amassed, processed, and saved has escalated exponentially, main to developing worries approximately information breaches, misuse, and the erosion of private privateness. Privacy and information safety rule's purpose to strike a sensitive stability among permitting innovation and safeguarding people' 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 is constrained to the reason for which it turned into obtained, and ensuring information accuracy and security. Additionally, those legal guidelines frequently supply people the proper to access, rectify, or delete their private statistics. Moreover, those rules make bigger past country wide borders, impacting agencies working internationally. Organizations should observe diverse local legal guidelines, main to the established order of worldwide information safety requirements. Furthermore, the effectiveness of such rules is based closely on enforcement, and government should have the ability and assets to pursue and penalize offenders adequately. In conclusion, privateness and information safety rules play a pivotal function in safeguarding people' rights and agree with withinside the virtual age. By fostering accountable information practices and conserving companies accountable, those rules make contributions to a more secure and extra stable virtual panorama for people and agencies alike. 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, Free Flow, International, Digital Economy, Stakeholders

I. Introduction

The transfer of cross-border data is most vital aspects 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 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 a present global digital world, internet-based advertisement and retailing, electronic payment systems and on-

ILE LEX SPECULUM
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

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 and to effectively tackle the issues of national security, intellectual property, and privacy, or to 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 that 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 DPDP Bill, 2022 but still such legislation has some lacunas like Clause 17 of the DPDP Bill, 2022[72] 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.

II. 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; it 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 individual privacy rights and facilitating data transfers for legal purposes[73]. Cross-border transmissions of data can benefit from a risk-based strategy, which can assist concentrate 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. It is crucial to create an impartial regulatory body with adequate funding to monitor international data flows. 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 very 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 prior to 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

[72] Amar Patnaik, *Looking at the cross-border data flow regime in the DPDP Bill 2022*, HINDUSTAN TIMES (July 13, 2023, 10:00 AM), https://www.hindustantimes.com/ht-insight/economy/looking-at-the-cross-border-data-flow-regime-in-the-dpdp-bill-2022-101680090578675.html.

[73] THE WORLD BANK, https://id4d.worldbank.org/guide/data-protection-and-privacy-laws (last visited July 13, 2023).

ILE LEX SPECULUM
VOLUME I AND ISSUE I OF 2023
APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

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[74]. 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, in order 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.

III. 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 in order 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)[75]. 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

[74] M. Danov, Data Analysis: Important Issues to Be Considered in a Cross-Border Context, UNIVERSITY OF EXETER (July 13, 2023, 10:00) AM), https://ore.exeter.ac.uk/repository/handle/10871/29567

[75] Vikram Jeet Singh, Kalindhi Bhatia and Prashant Daga, Privacy Week Series: Analyzing Cross-Border Data Transfer Mechanisms – Privacy Protection – India, MONDAQ (July 13, 2023, 6:00 PM), https://www.mondaq.com/india/privacy-protection/1276438/privacy-week-series-analyzing-cross-border-data-transfer-mechanisms#:~:text=It%20offers%20a%20

cryptography is weak to succeed on the international stage, and halts the progress of safeguarding data. In order 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 data, this strategy will boost the opportunity of the various stakeholders and enable a larger, broader atmosphere for cross-border data transfers amongst stakeholders.

IV. 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. Prior to utilizing or acquiring someone's personal information, it is a widely accepted practice to get that person's consent, and the DPDP Bill, 2020 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. In order to minimize ambiguity or wide phrasing, consent applications should be focused and specific. 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[76]. 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 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.

V. Cross-border Data Flow and Indian Digital Economy

[76] Bhavna Sharma, Dhawal Gupta & Ajay Singh Chauhan, Data Protection Standards For Cross Border Data Transfers In India: Suggestive Approaches And Way Forward, LIVELAW (July 13, 2023, 7:00 PM), https://www.dataguidance.com/opinion/india-best-practices-cross-border-data-transfers

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. Analysing 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[77], and from the growth trends, it could be denoted that 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. But 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 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.

With respect to 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 minimise 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 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 fulfil all the requirements of the legislation. However, on the other hand, the General Data Protection Regulation (GDPR)[78] adopted by Europe proved effective in protecting personal data and ensuring the cross-border data flow. Although 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.

VI. Approaches which 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 own 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

[6]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 ,(July 15, 2023, 10:00 https://timesofindia.indiatimes.com/blogs/voices/the-digital-personal-data-protection-bill-2022-panacea-or-pandoras-box/

[78] THE GENERAL DATA PROTECTION REGULATION(GDPR), https://gdpr-info.eu/ (last Visited July 13, 2023).

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 and 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[79] is quite unclear and it will require India to enter lethargic negotiations with numerous countries in order to successfully whitelist them thereby de-facto blacklisting the countries with unsuccessful or pending negotiations. Another lacuna in the DPDP Bill 2022, 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," this approach 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 seamless transfer of cross-border data[80]: Firstly, the Indian government must reframe the legislation which should define the word "adequate" 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 standardised 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.

VII. Conclusion

In conclusion, information safety for switch in India is a crucial problem that calls for cautious attention and powerful measures. The suggestion strategies mentioned on this challenge provide capacity answers to deal with the demanding situations related to information transfers, at the same time as making sure the privateness and safety of private statistics. The first proposed method, the enactment of complete information safety legal guidelines, is critical to set 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 additionally offer people with enforceable rights and remedies. Additionally, the established order of an impartial regulatory authority can make sure 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 far essential to make sure that those mechanisms are frequently reviewed and up to date to hold tempo with technological improvements and evolving privateness concerns. The subsequent steps in addressing information safety for

[79] Soumyarendra Barik, *Data Protection Bill approved by Cabinet: Content, concerns*, THE INDIAN EXPRESS (July 15, 2023, 11:09 AM), https://indianexpress.com/article/explained/explained-economics/data-protection-bill-approved-by-cabinet-content-concerns-8780035/

[80] DATAGUIDANCE, https://www.dataguidance.com/opinion/india-best-practices-cross-border-data-transfers (last visited July 15, 2023).

switch 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 align India's guidelines with worldwide norms, selling harmonized information flows. Furthermore, making an investment in technological answers consisting of encryption, anonymization, and stable information garage 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 make a contribution 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.

VIII. Reference

1. Anghrija Chakraborty, Ashima Obhan, Amar k Sundaram, Data Protection Laws Demystified (1st edition – 2021) Pg. 56.
2. Advocate Shruti Bist, Personal Data Protection Bill 2019 And Analysis OF Puttaswamy (1st edition – 2019) Pg. 11.
3. Simon Chesterman, Data Protection Law in Singapore (2nd edition- 2014) Pg. 345.
4. Pawan Duggal, Data Protection Law in India (2016th edition- 2016) Pg. 100.