VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CROSS-BORDER DATA FLOW IN INDIA: AN ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND GENERAL DATA PROTECTION REGULATIONS, 2016

- Shabih Fatima[1]

Abstract

This research paper explores the critical role of cross-border data flow in the global economy, focusing on India's evolving digital regulation. It examines the impact of India's Digital Personal Data Protection Act 2023 on international data transfer, comparing it to the European Union's GDPR. Key issues such as data privacy, protection, sovereignty, and the challenges businesses face in complying with international laws are discussed. The paper also delves into data flows' economic and societal implications, highlighting the need for international cooperation and the potential risks involved.

Introduction

In an era where data is as valuable as currency, the movement of this digital asset across international boundaries, known as cross-border data flow, has become a critical component of the global economy. This is particularly true for India, a burgeoning digital innovation hub home to over a billion people. With its rapidly expanding internet user base and booming IT sector, the nation's approach to managing cross-border data flow is a matter of national interest and a significant factor in the global data economy.

The cornerstone of India's digital regulation is the Information Technology Act of 2000, which sets the framework for electronic governance and security practices. However, newer regulations have been proposed as data privacy and cross-border data transfer have become more pressing. The Personal Data Protection Bill (PDP), inspired by the European Union's

[1] Student at Jamia Millia Islamia, New Delhi

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

https://www.ijalr.in/

General Data Protection Regulation (GDPR), aims to provide a more robust legal structure for data protection in India.

One of the critical features of the PDPA 2023 is its approach to transferring personal data outside India. The Act has relaxed data localization requirements compared to earlier legislation attempts, allowing cross-border data flow to certain countries and territories as notified by the central government. This indicates a shift from the previous stringent local storage or localization requirements, offering more flexibility in international data transfers. However, this flexibility is restricted, as only countries specified by the central government under the Act are permitted for such data transfers. The details of the criteria for notifying these countries and other data processing-related details are yet to be announced by the Data Protection Board of India. Proponents argue that this enhances data security and national sovereignty, while critics point to the potential impediments to the free flow of information that fuels the global digital economy.

Cross-Border Data Flow

Cross-border data flow is a cornerstone of the modern digital economy. It enables multinational corporations to operate efficiently by allowing them to transfer customer, operational, and financial data between different countries. For instance, a company based in the United States with operations in Europe and Asia relies on seamless data flow to coordinate its activities, manage supply chains, and offer customer services. [2]

Additionally, these data flows support the services of tech giants like Google, Facebook, and Amazon, whose business models depend on the global exchange of information and e-commerce. In social media and communication, cross-border data flow allows instantaneous connection and information exchange, making the world more interconnected than ever.

While the benefits are substantial, cross-border data flow raises several challenges and concerns. One major issue is data privacy and protection.[3] Different countries have varying regulations regarding data protection, like the General Data Protection Regulation (GDPR) in the European Union, which sets stringent rules on data handling and privacy. Companies

[2]Christopher Kuner, TRANSBORDER DATA FLOW AND PRIVACY LAW 3-22 (2013).
[3]Ira S. Rubeinstien, *Big Data: End of Privacy or a New Beginning?* 3 International Privacy Law Journal, Oxford University Press, 74, 2012.

operating across borders must navigate these diverse legal landscapes, ensuring compliance to avoid penalties and safeguard user data.

Another concern is data sovereignty. Some governments impose restrictions on data leaving their borders to maintain control over it, often citing national security or privacy reasons. This can lead to data localization, where companies must store and process data within the country of origin. Such practices can hinder the efficiency of global data flows, impacting services and increasing operational costs for businesses.[4]

International agreements and frameworks have been developed to address these challenges. Agreements like the US-EU Privacy Shield (now invalidated and under review for a new framework) aimed to facilitate data transfers while ensuring adequate data protection. Multilateral contracts under the World Trade Organization (WTO) and regional trade agreements often include provisions for digital trade and data flow, attempting to balance the free flow of data with privacy and security concerns.[5]

The economic implications of cross-border data flows are significant. They enable small and medium-sized enterprises (SMEs) to access global markets, leveraging cloud services and e-commerce platforms. This democratization of international trade can lead to economic growth, innovation, and increased competition.

Moreover, efficient data flow is crucial for emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT). These technologies rely on vast datasets, often sourced from multiple countries, to improve algorithms and services.

Beyond economics, cross-border data flows impact society at large. They facilitate cultural exchange and global collaboration in science and education. Researchers worldwide can share data and collaborate on projects, advancing knowledge and innovation. However, there are also concerns about cultural homogenization and the dominance of certain nations in the digital space, which can lead to imbalances in information flow and influence.

Looking ahead, the cross-border data flow landscape will likely evolve with technological advancements and changing regulatory environments. The increasing volume of data and the

[4] O Shane Balloun, *Cloud Computing…And the Practise of Law,* 37-APR. Wyo. Law, 32, 2014.
[5]Barbara Crutchfield George & Deborah Roach Gaut, *Offshore Outsourcing to India by US and EU Companies,* 6 U.C DAVIS BUS, L.J. 13 (2006).

development of new technologies will continue to drive the importance of these flows. At the same time, concerns over privacy, security, and data sovereignty will prompt further debate and potentially new regulatory approaches.

Digital Personal Data Protection Act, 2023

The Personal Digital Data Protection Act (PDPA) 2023 of India represents a significant development in the country's approach to digital data protection, with notable implications for cross-border data flow. The Act has been designed to replace Section 43A of the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which were India's prevailing data protection frameworks.

The PDPA 2023 is a principles-based legislation similar to the GDPR, governing data fiduciaries (data controllers), data processors, and data principals (data subjects). It applies to personal data collected digitally or digitized after being collected non-digitally, excluding data processed for personal or domestic purposes or aggregated personal data collected for research, which is not used for decision-making specific to a data principal. Notably, the Act only applies to entities outside India that monitor the behavior of data subjects within India, setting it apart from the GDPR's broader territorial scope.

The Act requires data fiduciaries to obtain consent for data processing, which should be free, specific, informed, unconditional, and unambiguous.[6] However, data fiduciaries may also process personal data for 'legitimate uses' such as fulfilling legal obligations, medical emergencies, public order breakdowns, and employment purposes.

The PDPA 2023 categorizes data fiduciaries into different brackets based on the volume and sensitivity of the personal data they handle. Significant data fiduciaries, those dealing with large volumes of individual personal data, have additional obligations, including appointing a data protection officer and conducting data protection impact assessments. Conversely, small-sized data fiduciaries and start-ups may be exempted from certain obligations.

Regarding data breach management, the Act mandates that all personal data breaches must be reported to the Data Protection Board and the affected data principals. This requirement is a

[6]The Digital Personal Data Protection Act, 2023, s. 15.

first for India and differs from the GDPR, which only requires notification of high-risk breaches.[7]

The PDPA 2023 marks a significant step in India's data protection landscape, particularly in its approach to cross-border data flow, consent mechanisms, and data breach notification requirements. Its full impact and effectiveness will become more apparent as the accompanying rules are issued and the Data Protection Board of India begins its operations.

The Digital Personal Data Protection Act of 2023 addresses the transfer of personal data across Indian borders in Section 16. This particular section concentrates on international data transfer, focusing on several key aspects:

- Section 16(1) empowers the central government to limit the transfer of personal data to foreign nations by issuing notifications for specified countries as it considers appropriate.[8]

- Section 16(2) integrates the DPDP Act with pre-existing legal frameworks by permitting the enforcement of current, more stringent data protection regulations.

In a global context, numerous advanced nations have established rigorous policies concerning cross-border data protection. The European Union's General Data Protection Regulation, commonly known as GDPR, outlines the conditions for transferring personal data from an EU member state to a non-EU country.

General Data Protection Regulations, European Union

The GDPR in Europe allocates an entire chapter to the regulations governing the protection of personal data across borders, imposing severe penalties for violations. These can include fines of up to €20 million or 4% of the company's global annual revenue from the previous year. The severity of these fines underscores the importance of adherence to these regulations.

Transferring personal data within the European Union requires that data handlers and processors enter a formal agreement. This agreement details the specific data involved, its nature, the duration, and the purpose of the processing.

When transferring data outside the EU to a non-EU nation, such actions fall under the scope of an 'Adequacy Decision.' This decision is a benchmark that ensures non-EU countries,

[7]The Digital Personal Data Protection Act 2023, s. 18 & s. 29.
[8]The Digital Personal Data Protection Act, 2023 s. 16.

territories, or international organizations provide data protection levels comparable to those in the EU.

If a favorable adequacy decision is established, personal data can be transferred from the EU to the corresponding country.

Within the framework of the GDPR, Data Controllers also have to adhere to specific measures for international data transfer. This includes compliance with corporate rules, particularly relevant for multinational companies. The EU has set forth standardized clauses and certification processes for international data transfer.[9]

Comparison of Personal Digital Data Protection Act, 2023 with the General Data Protection Regulations, European Union

1. Data Localisation and Transfer

The GDPR does not mandate data localization, allowing data transfer outside the EU to countries that ensure adequate data protection, or through mechanisms like Standard Contractual Clauses or Binding Corporate Rules.[10]

The DPDP Act has relaxed earlier data localization norms. It allows cross-border data transfer, but only to countries or territories notified as providing adequate protection by the Indian government. This approach is more restrictive than the GDPR and depends on government notifications.

2. Adequacy Decisions

The European Commission has the authority to determine whether a country outside the EU offers adequate data protection. Once a country is deemed sufficient, data can flow from the EU (and EEA) to that country without any further safeguard being necessary.

Like the GDPR, the DPDP Act relies on adequacy decisions made by the central government. However, the criteria and process for these decisions under Indian law are less precisethan the established procedures under the GDPR.

3. Transfer Mechanisms

[9]W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 Wash. Int'l L.J. 485 (2020).
[10] Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent, Jennifer Boling, and Amanda Sweenty, Law and Business Technology: Cyber Security & Data Privacy Update, 20 TENN.J. BUS. L. 1065, 1071 (2019)

Besides adequacy decisions, the GDPR offers alternative transfer mechanisms such as Binding Corporate Rules (BCRs) for multinational corporations, Standard Contractual Clauses (SCCs) for data transfers between organizations, and exceptions for specific situations.

The specific mechanisms for data transfer under the DPDP Act, beyond adequacy decisions, are more explicitly outlined than in the GDPR. The Act's future rules and interpretations by the Data Protection Authority of India might provide more clarity.

4. Government Access to Data

The GDPR strictly limits government access to personal data, requiring it to be necessary and proportionate. The EU strongly emphasizes protecting data from undue access by authorities, including foreign governments.[11]

There are concerns that the DPDP Act could allow broader government access to data, especially in the context of national security or public interest. This aspect of the Act has been a point of contention and differentiates it from the GDPR's approach.

5. Protection Level and Scope

Recognized as one of the strictest data protection laws globally, the GDPR provides comprehensive rights to individuals and imposes significant obligations on data processors and controllers.

While the DPDP Act marks a significant step in strengthening data protection in India, it is generally perceived as less stringent than the GDPR. Its focus is more on enabling data flow while balancing privacy rights.

6. Extra-territorial Scope

The GDPR has a broad extraterritorial scope, applying to any organization that processes the data of individuals in the EU, regardless of where the organization is based. [12]

[11] MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS 30 (March 2016).
[12] W. Gregory Voss, Internet, New Technologies, and Value: Taking Share of Economic Surveillance, 2017 U. ILL. J.L. TECH. & POL'Y 469, 472 (2017).

The DPDP Act's extraterritorial scope needs to be clarified compared to the GDPR. It is primarily aimed at data processing within India and does not explicitly extend to foreign entities processing data of Indian residents.

In summary, while the GDPR and the DPDP Act 2023 aim to protect personal data and regulate its flow across borders, the GDPR is more comprehensive and established in its approach, especially regarding transfer mechanisms, government access to data, and extraterritorial applicability. The DPDP Act, on the other hand, is a significant step for India but is still evolving in terms of its operational details and global alignment.

Challenges within the DPDP Act, 2023

The primary concern revolves around data privacy and security. Ensuring the protection of personal information as it crosses borders is a complex task, compounded by varying international standards.

The complexity and cost of compliance with many international laws pose significant challenges for businesses, especially SMEs. The Indian IT sector, which often caters to clients from multiple countries, navigates this intricate legal landscape.

Moreover, data sovereignty has become a topic of international tension. Countries are increasingly asserting their right to govern the data generated within their borders, leading to potential conflicts in cross-border data policies.

The Digital Personal Data Protection Act 2023 of India, while a significant step in updating the country's data protection framework, has been met with some criticism, particularly in the context of cross-border data flow:

1. Relaxed Data Localization Requirement

The Act has relaxed the data localization requirements compared to previous iterations of data protection bills. This means personal data can be transferred from India to certain countries or territories that the central government will specify. Critics argue that this could lead to potential risks associated with transferring personal data to jurisdictions with varying levels of data protection, potentially undermining the privacy and security of Indian users' data.

2. Lack of Clarity on Adequate Jurisdiction

The Act allows cross-border data flow only to countries deemed 'adequate' by the Indian government, but the criteria for determining adequacy are not clearly defined. This ambiguity could lead to uncertainty for businesses and data fiduciaries who engage in international data transfers, as they may need help to anticipate which countries will be deemed adequate or the standards used to make these determinations.

3. Potential Impact on International Business Operations

The Act's approach to cross-border data flow might pose challenges for international businesses, particularly those relying on global data transfer. Companies need to establish complex compliance mechanisms to adhere to these regulations, potentially increasing operational costs and affecting business efficiency.

4. Concerns about International Reciprocity and Cooperation

The Act's approach to cross-border data flow might raise concerns about reciprocity and international cooperation in data governance. Countries might respond with similar restrictions on data flow from their jurisdictions to India, which could lead to a fragmented global data regime, affecting multinational operations and international digital trade.

5. Risk of Data Sovereignty

Allowing the central government to dictate data flow to specific countries could lead to data sovereignty issues. This might result in data being stored in jurisdictions where the Indian government has more influence or control, which could be perceived as a move away from a free and open internet.

In summary, while the Digital Personal Data Protection Act 2023 represents a significant overhaul of India's data protection regime, its provisions related to cross-border data flow have raised concerns about potential risks to data privacy, operational challenges for businesses, and broader implications for international data governance norms.

Conclusion

While the GDPR was influenced by the EU Charter of Fundamental Rights and the earlier Data Protection Directive, the DPDPA is a legal embodiment of the fundamental right to privacy declared by the Supreme Court of India in 2017.

The DPDPA introduces the Data Protection Board, a new regulatory body. Unlike the broader regulatory mandate of European (and UK) supervisory authorities, which includes rulemaking and administrative tasks, the Data Protection Board mainly addresses grievances and imposes penalties for data breaches.

Under the DPDPA, the Indian government holds all rule-making authority and prefers simplicity and business-friendliness. This approach suggests a less detailed, more principle-driven framework in India, leading to potentially greater interpretational leeway and uncertainty.

The DPDPA imposes much steeper penalties than current Indian laws, with fines up to INR 250 crores (approximately GBP 25 million) under the new system. These fines are punitive, not compensatory, and go to India's Consolidated Fund. Additionally, the DPDPA introduces unique Indian features, such as electronic alternate dispute resolution and voluntary commitments by data fiduciaries. It also allows the Government to block public access to information (including websites and apps) used by data fiduciaries to offer services in India for repeated violations.

The DPDPA significantly diverges from the existing SPDI Rules, marking a significant advancement in India's data protection landscape. In a context where setting examples for compliance with new regulations is crucial, and website bans are not rare; entities should anticipate more assertive, proactive regulation. This extends beyond written laws to active oversight by the Data Protection Board and sector-specific regulators like the Reserve Bank of India.

While the DPDPA has been passed into law, it still needs to be in effect. The specifics of this legislation will be clarified in upcoming rules that are still to be released. It is anticipated that the DPDPA will be rolled out gradually.

While the DPDPA shares certain concepts and principles with the GDPR, making it somewhat familiar to international organizations versed in European and UK compliance, it is not a replica of the GDPR. There are significant distinctions that require thorough

consideration. This highlights that a single approach sometimes applies to global data protection compliance for multinational companies.