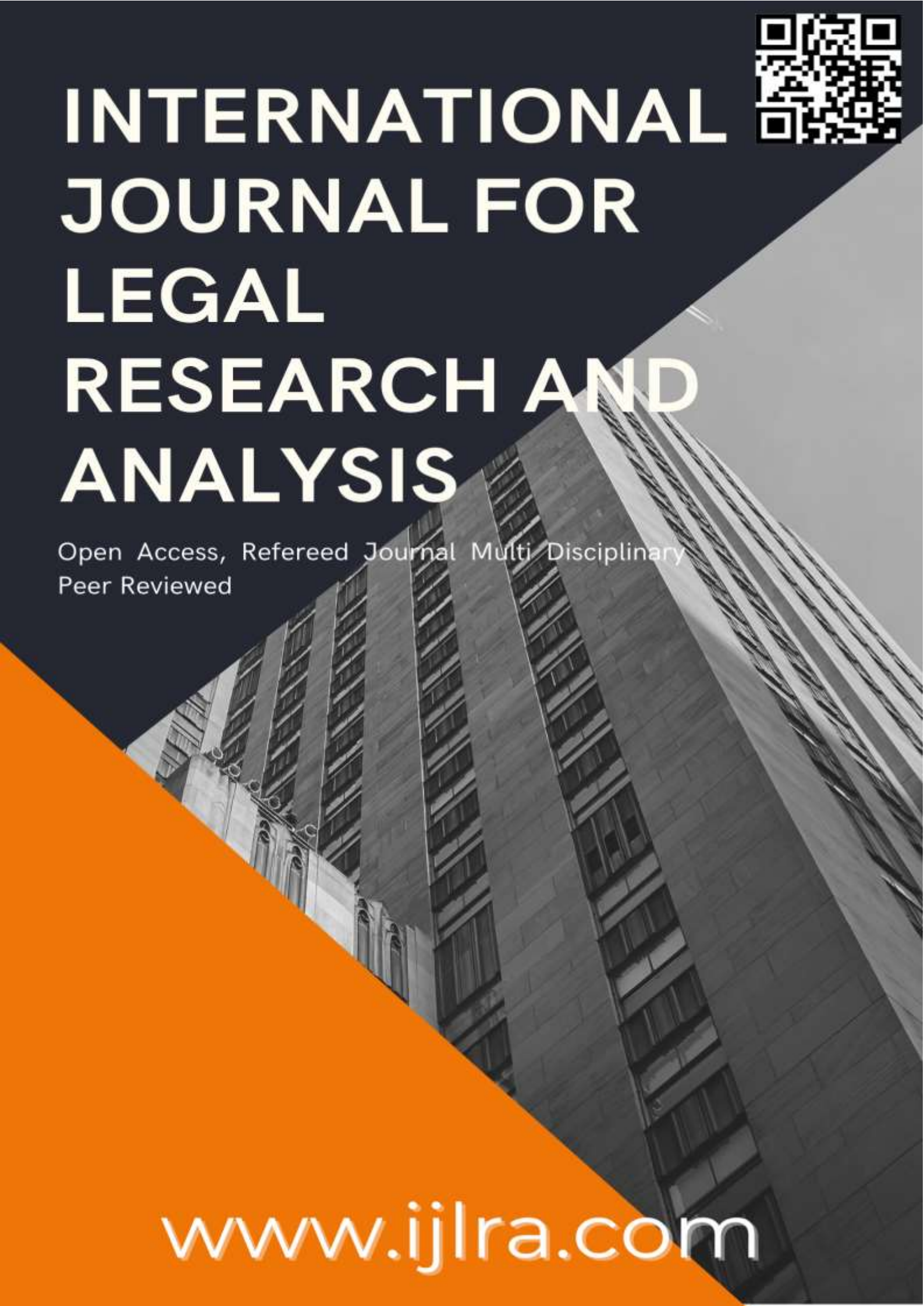
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CROSS-BORDER DATA FLOW AND LEGAL FRAMEWORK IN INDIA

AUTHORED BY - HARI PARKASH & KHUSHAL SAINI

Abstract

In the rapidly evolving digital age, cross-border data flow has emerged as a critical area of legal, economic, and geopolitical concern. As India positions itself as a global digital hub, the governance of data transfers across national boundaries becomes essential to ensuring privacy protection, national security, and economic competitiveness. This paper examines the conceptual and legal framework surrounding cross-border data transfers in India, highlighting the country's legislative evolution, particularly the enactment of the Digital Personal Data Protection Act, 2023. It explores key regulatory challenges such as data localization, enforcement limitations, and international compliance obligations, while comparing India's approach with international models like the EU's GDPR, the US's sectoral regime, and China's state-centric controls. Judicial perspectives and constitutional implications are critically analyzed to understand how India's legal system reconciles individual privacy with sovereign and economic interests. The paper concludes by offering comprehensive policy recommendations aimed at balancing innovation, global interoperability, and domestic safeguards. Through this interdisciplinary inquiry, the study contributes to the discourse on building a rights-respecting, transparent, and accountable data governance framework in India.

ISSN: 2582-6433

Table of contents

ISSN: 2582-6433

- **Challenges in Regulating Cross-Border Data Flow in India**

8.1. Absence of Adequacy Standards

8.2. Executive Overreach and Regulatory Independence

8.3. Undefined Sensitive and Critical Data Categories

8.4. Weak Enforcement and Judicial Remedies

8.5. Trade and Investment Barriers

8.6. Cybersecurity and Jurisdictional Limitations

8.7. Public Awareness and Industry Readiness

- **The Way Forward – Recommendations for India**

9.1. Adequacy Framework

9.2. Independent Data Protection Authority

9.3. Contractual and Regulatory Clarity

9.4. Categorization of Sensitive Data

9.5. International Collaboration and Diplomacy

9.6. Cybersecurity Infrastructure and Enforcement

9.7. Capacity Building and Awareness

- **Conclusion**

ISSN: 2582-6433

Introduction

In the modern digital age, data has become a strategic asset that affects global economic patterns, sparks new ideas, and changes how governments work. As countries quickly move to digital, the flow of data across countries, also known as Cross-Border Data Flow (CBDF), has become quite important. CBDF stands for the electronic transfer of data across borders, which makes it easier for businesses, governments, schools, and people to work together from afar.[1] The open and safe movement of data has become necessary as more and more people use cloud computing, social media, international commerce, and digital financial services.

But the easy flow of data raises big worries about privacy, national security, regulatory control, and digital sovereignty. Governments all across the world, including India, are trying to find a balance between protecting people's private information and letting information flow freely, which is important for the digital economy.[2] This contradiction has caused many legislative methods to emerge, such as data localisation requirements, limits on international transfers, and bilateral or multinational frameworks to control CBDF.

India's digital environment is growing quickly, but it is also dealing with the problems that come with not having a full data security system until recently. The Digital Personal Data Protection Act, 2023, is a big step forward for India in its efforts to find a balance between protecting personal data and making it easier to share it.[3] This new law comes after other laws, such the Information Technology Act of 2000, and court decisions, like the Puttaswamy case, which recognised privacy as a basic right.[4]

This study seeks to investigate the development, obstacles, and future possibilities of the legislative framework regulating cross-border data movement in India. It looks at India's place in the global legal framework for data governance, compares it to important international models, and checks to see whether the country's rules are good enough and can be enforced. The paper's scope encompasses:

- A historical and theological examination of Indian legislation on data privacy and international data flows.

[1] Greenleaf, G. (2022). *Global data privacy laws 2022: Despite COVID delays, 157 laws show GDPR dominance*. Privacy Laws & Business International Report, (172), p. 14
[2] Chander, A. & Lê, U. P. (2015). *Data Nationalism*. Emory Law Journal, 64(3), pp. 677–739
[3] Government of India. (2023). *The Digital Personal Data Protection Act, 2023*. Ministry of Electronics and Information Technology, New Delhi, p. 6
[4] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India, (2017) 10 SCC 1

ISSN: 2582-6433

- A comparative legal analysis of significant jurisdictions, including the European Union, the United States, and China.
- Assessment of judicial interpretations in Indian courts concerning data privacy and digital autonomy.
- Suggestions for changes to policies and making them the same over the world.

The goal is to have a legally sound, analytically rich, and policy-relevant discussion on how India may regulate CBDF while still following the Constitution, being competitive in the economy, and keeping control over technology.

Theoretical Framework and Methodology

To understand how cross-border data movement is regulated, you need a framework that looks at both legal theory and practical governance issues. This section delineates the theoretical framework and methods used in this article to assess India's legislative reaction to cross-border data transmission.

2.1. Theoretical Framework

The research is based on techno-legal realism, a legal theory that looks at how law, technology, and society affect one other. Techno-legal realism, on the other hand, stresses the necessity of understanding legal norms in light of technology changes, policy needs, and institutional capability. Strict legal positivism sees law as a collection of rules that are not connected to social and technical contexts.[5]

Techno-legal realism helps us comprehend how laws work when there are digital disruptions, international trade talks, geopolitical conflicts, and privacy concerns. This is important for cross-border data regulation. It enables this article to critically evaluate whether India's data protection framework—both current and proposed—sufficiently handles the intricate realities of data localisation, cybersecurity, and monitoring within a globally interconnected digital economy. [6]

The study is also shaped by the idea of digital constitutionalism, which says that human rights and democratic ideals should be included into the digital infrastructure of government. This is

[5] Solove, D. J. (2021). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, p. 41
[6] Belli, L., & Zingales, N. (2017). *Platform regulations: Balancing freedom of expression and privacy in the digital age*. Internet Governance Forum, p. 23

ISSN: 2582-6433

particularly pertinent after the Supreme Court of India's acknowledgement of the right to privacy as a basic right in Justice K.S. Puttaswamy v. Union of India.[7] The case not only set the stage for privacy-focused laws, but it also made the state more accountable for how it handles data.

2.2. Methodology

This study utilises a doctrinal legal research technique, often referred to as the "black letter" approach. It entails a thorough analysis of legislation, court rulings, policy documents, and authoritative commentary. We look at important laws like the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 to find principles, norms, and regulatory procedures that apply to data transfers across borders. [8]

The research also looks at Indian sources and compares them to foreign models, especially:

- The General Data Protection Regulation (GDPR) of the European Union,
- The United States' framework for sectors and surveillance,
- The laws of the People's Republic of China that deal with cybersecurity and data export restriction.

We look at primary and secondary sources to see whether they are consistent, enforceable, and follow international rules. To learn about global norms and how India's policies fit in, reports from groups like the OECD, APEC, UNCTAD, and the World Economic Forum have been used.[9]

The study is both descriptive and analytical. It explains the legal situation, compares it to the best practices throughout the world, and then criticises it using constitutional principles and regulatory theory. The main goal is to provide practical legislative changes and policy solutions that protect people's rights while also making sure India stays competitive in the digital world and safe.

Evolution of Data Protection and Privacy Laws in India

3. How India's laws on privacy and data protection have changed over time

India's legal path to protecting data and privacy has changed from a patchwork of regulations

[7] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India, (2017) 10 SCC 1, at p. 42
[8] Information Technology Act, 2000, and Digital Personal Data Protection Act, 2023, Government of India
[9] UNCTAD. (2021). *Data Protection and Privacy Legislation Worldwide*. United Nations Conference on Trade and Development, p. 5

ISSN: 2582-6433

for different sectors to a more organised system. The Digital Personal Data Protection Act, 2023, is the most recent step in this process. This change is a result of changes in technology, judicial activism, and worldwide regulatory tendencies. To understand how the nation handles cross-border data flow, it's important to know this trajectory.

3.1. The IT Act of 2000 was the first law to deal with this issue

The Information Technology Act of 2000 was the first law in India to include data protection. The Act's main emphasis was on cybercrime and electronic commerce, although it did include certain protections for digital data:

- Section 43A made companies responsible for not using "reasonable security practices" while managing sensitive personal data, which resulted to unlawful loss or gain.[10]
- Section 72A made it a crime to share personal information without permission if it was collected while providing services under a contract.[11]
- But the law didn't clearly define "sensitive personal data," and the way it was enforced wasn't very strong. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 tried to fix these problems, however they only applied to businesses, not to government agencies.[12]

3.2. The Courts' Acknowledgement of Privacy as a Basic Right

The Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India (2017) was a turning point in Indian data law. The nine-judge bench unanimously agreed that the right to privacy is a basic right under Article 21 of the Constitution.[13]The Court stressed that privacy involves the right to choose how your information is used and that the state must prove that it has a good reason to handle data using a three-part test:

- Legality,
- A valid goal of the state, and
- Proportionality

This ruling set the constitutional groundwork for broad data protection laws in India. It forced the government to write rules that protect privacy as a basic right and stress due process and minimum interference with personal life.

[10] Information Technology Act, 2000, §43A
[11] Ibid., §72A
[12] Ministry of Electronics and Information Technology. (2011). *IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, Rule 3
[13] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India, (2017) 10 SCC 1, at p. 42–45

ISSN: 2582-6433

3.3. Draughting of Data Protection Bills and Changes in Policy

After Puttaswamy, the government created the Justice B.N. Srikrishna Committee. This group gave the government a draft of the Personal Data Protection Bill in 2018. The Bill brought in important privacy rules such limiting the purpose of data collection, limiting the amount of data collected, getting user agreement, and limiting the amount of time data is stored.[14] The 2019 version, on the other hand, watered down several parts, giving the state broad authority to use personal data for "public order" or "security of the state."

Civil society, industrial players, and foreign observers all strongly criticised the Bill for not having enough protections and too many exceptions. The Bill was completely taken off the table in 2022, which showed that the administration wanted to replace it with a "simplified" version.

3.4. The Digital Personal Data Protection Act of 2023

The Digital Personal Data Protection Act was passed in August 2023. The Act covers personal data that is acquired online or digitised offline and then processed in India. It also covers data that is processed outside of India if it is relevant to products or services supplied in India. It sets rules for "data fiduciaries" and "data processors," such as getting permission, stating the purpose, limiting the amount of data collected, and taking reasonable steps to protect it.[15]

The Act allows cross-border transfers to nations that the Central Government has informed about, which is a change from the previous data localisation rules. But the Act also lets the government handle things without following the rules, which has brought up worries about state spying and a lack of court control again.

The Act is a big step in the right direction, but it's still contentious since it doesn't include clear rights like the freedom to move data or the right to be forgotten. It also doesn't have an independent data protection body; instead, it has a Data Protection Board of India that is controlled by the government.

[14] Srikrishna Committee. (2018). *Report of the Committee of Experts on Data Protection*, Government of India, p. 22
[15] Digital Personal Data Protection Act, 2023, §3(b)–(d)

ISSN: 2582-6433

Cross-Border Data Flow: International Legal Framework

As the digital economy grows and crosses national borders, it has become a major issue in global governance to figure out how to control the movement of personal data across borders. Different countries have made different laws to control the transmission of data across borders. These laws typically reflect different goals, such as protecting privacy, opening up commerce, protecting national security, and protecting digital sovereignty. This part talks about important international models that affect the legal discussion over cross-border data flow and gives an idea of the global norms that India has to follow.

4.1. The GDPR Model for the European Union

The European Union's General Data Protection Regulation (GDPR), which went into effect in 2018, is the most important and comprehensive data protection law in the world. It makes it very hard to move data outside of the European Economic Area (EEA) and comes up with the idea of "adequacy decisions," which means that the European Commission says that a third country has the same degree of data protection. [16]

Chapter V of the GDPR says that data may only be sent to a country that is not in the EEA if:

- The nation has gotten an adequate decision, or
- Standard contractual clauses (SCCs), binding corporate regulations (BCRs), or particular derogations give the right level of protection.

The GDPR applies to every organisation that handles personal data of EU citizens, no matter where they are located. This has big effects for Indian companies who work with data from the EU.

The Court of Justice of the EU (CJEU) made the Schrems I and II rulings, which made the rules for legal data transfer even stricter. The EU-U.S. Safe Harbour and Privacy Shield frameworks were thrown out because they didn't do enough to safeguard EU residents from U.S. surveillance laws.[17] These instances show that data transfers need to come with rights that can be enforced and legal remedies.

[16] European Parliament and Council. (2016). *General Data Protection Regulation*, Regulation (EU) 2016/679, Chapter V, Art. 45–50

[17] Court of Justice of the European Union. (2020). *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18

ISSN: 2582-6433

4.2. United States: A framework based on sectors and surveillance

The GDPR is different from the US, which has a sector-specific and self-regulatory approach to data protection. The Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA) are examples of laws that control some areas. Private companies, on the other hand, generally depend on privacy policies and contractual standards.[18]

The U.S. doesn't have a federal-level comprehensive data protection legislation, which makes it harder for it to claim that it meets the GDPR's standards. The Cloud Act (2018) also lets U.S. law enforcement authorities access to data that American corporations keep in other countries, which is a big deal in the privacy debate throughout the world.[19]

Even though there are these worries, the U.S. still strongly supports the free flow of data via global trade groups like the G20 and WTO. The USMCA and CPTPP are two examples of bilateral and multilateral trade agreements that make it illegal to store data in one country and encourage data transfers across countries.[20]

4.3. APEC: Cross-Border Privacy Rules (CBPR)

The Asia-Pacific Economic Cooperation (APEC) came up with the CBPR System to provide member economies a way to protect their privacy that is both voluntary and works with other systems. It stresses responsibility and lets businesses certify that they are following privacy standards on their own, as long as a third party checks it.[21]

CBPR is less strict than the GDPR, but it is more flexible and trade-friendly. It is becoming more popular in Japan, Singapore, and South Korea. India is not a member of APEC and does not take part in CBPR. However, people in India who work in trade and policy regularly talk about the model as a possible way to balance privacy with economic interests.

4.4. OECD Guidelines and Global Standards

The Organisation for Economic Co-operation and Development (OECD) has also set up

[18] Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law* (6th ed.). Aspen Publishers, p. 78
[19] U.S. Congress. (2018). *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, Public Law No. 115–141, p. 232
[20] USTR. (2020). *United States-Mexico-Canada Agreement*, Chapter 19 (Digital Trade), Art. 19.11
[21] APEC Secretariat. (2015). *Cross-Border Privacy Rules System*, Policy Paper, p. 3

ISSN: 2582-6433

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, amended in 2013). These guidelines stress:

- Limitations on collection,
- Purpose definition,
- Limitations on use,
- Individual involvement, and
- Responsibility.[22]

The OECD principles are not legally obligatory, but they have had an impact on many national legislation and have encouraged privacy regimes to work together. They provide a soft-law way to get national laws to agree without making them all the same.

India's Approach to Cross-Border Data Transfers

5. India's Way of Moving Data Across Borders

India's strategy for regulating cross-border data transfers has been influenced by changing national interests, court actions, and a growing role in global commerce and technological networks. India, as a significant digital market, has switched between regulations that require data to stay in the country and policies that allow it to move freely. This is because people are becoming more concerned about privacy, cybersecurity, and digital sovereignty. This part looks closely at India's stance on cross-border data transfers in light of its current and future legislative environment.

5.1. Early Uncertainty According to the IT Act and the SPDI Rules

Before India passed comprehensive data protection laws, it used Section 43A of the Information Technology Act, 2000, and the SPDI (Sensitive Personal Data or Information) Rules, 2011, to control the movement of data.[23] Rule 7 of the SPDI Rules stated that cross-border transactions were only acceptable if:

- The receiver made sure that the "same level of data protection" was in place as the Indian system, and
- The transfer was essential to carry out a contract or was done with permission.[24]
- These criteria were not well defined and were not often enforced, which made the law

[22] OECD. (2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, p. 12
[23] Information Technology Act, 2000, §43A
[24] Ministry of Electronics and Information Technology. (2011). *SPDI Rules*, Rule 7

ISSN: 2582-6433

unclear. The Rules also only apply to "body corporates," which meant that government agencies and law enforcement were not subject to the same rules. This left a hole in the rules and made many worry about governmental overreach and monitoring, particularly after news of foreign intelligence programs like PRISM and domestic projects like CMS (Central Monitoring System).

5.2. Fight for Data Localisation and Sovereignty

As digital commerce and finance platforms grew, the discussion in India over cross-border data transfer became more heated. The Justice Srikrishna Committee (2018) suggested limiting data transfer by making sure that at least one copy of all personal data is kept in India and making "critical personal data" obligatory localisation.[25] People saw this as a reaction to the rise in cyber dangers and worries about spying by foreign governments.

After then, a number of sectoral regulators suggested localisation:

- In 2018, the Reserve Bank of India (RBI) said that all payment system data had to be kept in India.[26]
- The Draft E-commerce Policy (2019) pushed for severe rules on where customer data might be stored.
- The Draft Non-Personal Data Governance Framework (2020) suggested that communities should control anonymised datasets and that they should be kept within national boundaries.

But these steps made global corporations and trade partners, especially the United States, angry. They said that forced localisation boosts prices, stifles innovation, and makes it harder for businesses to operate throughout the world.[27]

5.3. Digital Personal Data Protection Act, 2023 — A Move Towards More Freedom

The Digital Personal Data Protection Act, 2023, changes the way data is transferred across borders from a strict localisation approach to one that the government must notify. According to Section 16 of the Act, the Central Government may provide personal data to nations or regions that it has deemed adequate and in the national interest.[28] This methodology is similar

[25] Srikrishna Committee Report. (2018). *A Free and Fair Digital Economy*, Government of India, p. 56
[26] Reserve Bank of India. (2018). *Storage of Payment System Data*, Notification No. RBI/2017-18/153
[27] USTR. (2021). *National Trade Estimate Report on Foreign Trade Barriers*, p. 199
[28] Digital Personal Data Protection Act, 2023, §16(1)dAQ

ISSN: 2582-6433

to the European Union's adequacy framework, however it is not clear or subject to judicial scrutiny.

This is a shift from previous localisation rhetoric, but it brings up problems about what "adequate" means, what role reciprocal agreements play, and how much protection there is in the destination countries. Critics also say that the rule might make it easier for the government to spy on people without their knowledge, which goes against the very privacy it is meant to safeguard.

5.4. Interventions by the courts and policy

After the Puttaswamy case, judges have said that any governmental action using data must be proportionate, limited to a specific goal, and as less intrusive as possible.[29] The Supreme Court has said that privacy rules must be in line with the Constitution, which has an effect on data transmission rules. India's involvement in groups like the G20, OECD, and Bilateral commerce Agreements (BTAs) has also pushed it to follow international data transmission rules more rigorously, particularly to get more investment and make sure that digital commerce is legal.

To sum up, India's laws for moving data across borders are changing. The path shows a balance between privacy and security on one side and economic freedom and working together with other countries on the other. We don't know yet whether the incoming government can maintain this balance.

Comparative Analysis: India vs. Global Models

6. A comparison between India and other countries' models

The way the law handles cross-border data transfers is quite different in different places. India must balance global best practices with its own needs as it works on its regulatory framework. This section compares India's approach to global data protection models, focussing on important concepts including adequacy, consent, localisation, and enforcement mechanisms. The models it looks at most closely include the EU, the U.S., and APEC.

6.1. Legal Basis for Transferring Data Jurisdiction India's Legal Basis for Cross-Border

Transfer Countries and territories that the government has notified about under the Digital

[29] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at p. 78–82

ISSN: 2582-6433

Personal Data Protection Act, 2023 (Section 16).European Union (GDPR): Adequacy determinations, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and specific permission under tight circumstances. The US There isn't a single legislation that governs data transmission; instead, there are rules for each industry and trade agreements. The focus is on protecting contracts.[30] APEC (CBPR system): A model for voluntary self-certification that must be checked by a third party.[31]

India has a hybrid model: it maintains discretion via official notifications, but there is no clear method for judging sufficiency or judicial review. The EU, on the other hand, has a thorough adequacy framework based on rights, whereas the U.S. has models focused on the market and commerce.

6.2. The Importance of Consent and User Rights

The GDPR requires that people provide their informed, clear permission, and that they have to choose to do so. Users also have considerable rights, such as the right to move their data, fix it, and delete it.[32]

The Digital Personal Data Protection Act of 2023 in India says that "free, specific, informed, unconditional, and unambiguous consent" is needed before processing personal data.[33] But the legislation is not as strong when it comes to enforcement and accountability, mostly because of the broad state exclusions in Section 17 and the few remedies available to individuals.

Also, India doesn't have the GDPR-like rights of data portability and automated decision-making redress, which makes it harder for people to manage cross-border transfers.

6.3. Localism and Independence Worries

India has always been in favour of data localisation, especially in banking and e-commerce. This is similar to what is happening in China and Russia, but quite different from what is happening in the U.S., EU, and APEC, which all support interoperable standards and the free movement of data with confidence.[34]

[30] Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law*, 6th ed., Aspen Publishers, p. 79–83
[31] APEC. (2015). *CBPR Policy Paper*, p. 5
[32] GDPR, Arts. 12–22
[33] Digital Personal Data Protection Act, 2023, §6
[34] USTR. (2020). *Digital Trade in the U.S. and Global Economy*, p. 14–17

ISSN: 2582-6433

The RBI's need for payment data to be stored in India and the new e-commerce policy show that India is still strategically interested in keeping digital sovereignty. On the other hand:

- Member states of the EU may transfer data freely between them.
- Through trade talks, the U.S. actively tries to stop localisation.
- The APEC CBPR promotes data flows via self-certification instead of storage mandates.

India's move away from mandated localisation under the DPDP Act is more in line with global trade rules, but it raises doubts about whether there are enough protections in place.

6.4. Enforcement and Institutional Framework

India's regulatory system has too many executives and not enough independent institutions. The GDPR approach, on the other hand, has significant regulatory monitoring and a system for people to get their rights back. The U.S. system has minimal government monitoring but strong enforcement of contracts.

6.5. Compatibility with global trade and interoperability

As digital trade becomes more important to global business, India's changing data legislation has to make sure that different systems can work together. The DPDP Act hints at making things work together throughout the world, but the absence of explicit adequacy criteria, worries about governmental spying, and unclear rules are still problems.

India must do the following to become a trusted data partner:

- Clear standards for adequacy;
- Clear rules for how states may get to data;
- Works with big rules like GDPR and CBPR;
- Trade agreements that recognise each other's data protection systems.

Challenges in Regulating Cross-Border Data Flow in India

7. Problems in regulating the flow of data across borders in India

India's goal of becoming a global digital powerhouse comes with complicated regulatory problems related to how cross-border data transfers are managed. Even though the Digital Personal Data Protection Act, 2023 (DPDP Act) is already law, there are still many problems with the way it works, the way it is set up, and the way it is thought about. This part talks about

ISSN: 2582-6433

the main legal, technical, and institutional problems that make it hard to enforce and regulate in India.

7.1. No Clear Adequacy Framework

Section 16 of the DPDP Act gives the Central Government the right to allow data transfers to "notified countries or territories."[35] But it doesn't have a defined method for evaluating sufficiency as the GDPR does. The rules for deciding what is adequate are still not clear. These include the legal standards, enforcement capabilities, and surveillance legislation of a foreign jurisdiction.

This lack of clarity makes it harder for Indian data fiduciaries and data principals to be sure about the law. It also hurts India's credibility in bilateral trade talks, as other countries may want proof-based evaluations and protections that work both ways.

7.2. Executive Discretion and Lack of Independence from Regulations

The executive sets up and runs India's Data Protection Board under Section 18 of the DPDP Act. This is different from the European Union's autonomous Data Protection Authorities.[36] This makes people worry about:

- Political power over choices on enforcement;
- Insufficient safeguarding of people' rights against governmental monitoring;
- There is no judicial monitoring in important regulatory procedures like country notifications or exemption rulings under Section 17.
- This kind of executive power makes it harder to maintain the balance of power under the Constitution, particularly in light of the Puttaswamy decision, which says that state action must be fair and clear when it comes to privacy.[37]

7.3. Unclear Classification of "Critical Data"

The previous versions of the data protection law required "critical personal data" to be stored in the same place. However, the final version of the DPDP Act does not include this word at all.[38] There is no definition or categorisation system for sensitive or essential data, which creates a regulatory gap, particularly in fields like:

[35] Digital Personal Data Protection Act, 2023, §16
[36] Ibid., §18
[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[38] Srikrishna Committee Report, (2018), p. 60–63

ISSN: 2582-6433

- National security and defence,
- Fintech and financial services,
- Genomic and health information.

This lack of regulation makes it more important to follow sectoral recommendations (such those from RBI, IRDAI, or MeitY), which makes compliance more difficult and creates uncertainty for global service providers.

7.4. Weak Enforcement System

The DPDP Act says that people may be fined, but it doesn't say how much.

- A personal right to take action;
- A well-defined process for getting justice for cross-border damages;
- If there are systematic breaches, there should be rules for class-action lawsuits or public interest lawsuits.

  On the other hand, the GDPR lets people go directly to Data Protection Authorities or courts to protect their data rights.[39] In India, the dependence on state-controlled enforcement without independent redressal mechanisms diminishes confidence in the regulatory framework.

7.5. Problems with Trade and Investment Interests

India's prior focus on data localisation, which was based on digital sovereignty, has been criticised by trade partners.For example:

- The U.S. Trade Representative (USTR) has called India's requirements for storing data trade obstacles;
- Restrictions on the flow of data have become major issues in FTA talks with the EU and the UK;
- India's ability to take part in regional digital commerce ecosystems is limited by the fact that it doesn't follow rules like CBPR.

It is still a difficult legislative task to find a balance between protecting data and encouraging cross-border investment and innovation.

7.6. Problems with cybersecurity and cross-border jurisdiction

Cyber breaches may happen during cross-border data transfers, particularly when data is

[39] GDPR, Art. 77–79

ISSN: 2582-6433

housed or processed in countries with weak cybersecurity legislation. India's lack of strong mutual legal assistance treaties (MLATs) and limited ability to execute laws outside of its borders makes it hard to investigate and punish these kinds of crimes.

Furthermore, cloud computing, blockchain, and data mirroring technologies make it harder to figure out where data is stored, which makes it practically difficult to enforce domestic data protection rules across borders without help from other countries.

7.7. People don't know enough about it and the industry isn't ready

Even if the law has changed, most people in India still don't know much about data rights. Most internet consumers don't know how their data is handled, stored, or sent.[40]Moreover, small and medium-sized businesses (SMEs) have high compliance expenses, particularly when it comes to keeping up with changing rules around cross-border data transfers.

This leads to poor compliance, ineffective consent, and a general lack of readiness among stakeholders, especially when there aren't any initiatives to increase capacity or financial incentives.

Conclusion of Problems

India's rules for moving data across borders are still being worked out. The DPDP Act is a good start, however the law's success hinges on:

- The growth of a strong system of institutions and courts,
- Clear standards for adequacy and rules for compliance,
- Clear executive actions that can be checked by the courts.

Only then can India set up a system for transferring data that respects rights, encourages innovation, and works with other countries.

The Way Forward – Recommendations for India

8. The Next Steps: Suggestions for India

India wants to be a trusted centre for data processing and digital innovation. To do this, its laws and rules for cross-border data flows need to go beyond baseline compliance and become the best in the world. This section's suggestions are meant to help create a data transfer system that

[40] USTR, (2021). *Foreign Trade Barriers Report*, p. 198–201

ISSN: 2582-6433

respects rights, encourages innovation, and works with other countries, all based on constitutional ideals and technical foresight.

8.1. Create a Clear and Principles-Based Adequacy Framework

India has to set up a formal adequacy assessment system that follows international standards, notably the GDPR. This framework needs to:

- Be open and ask the people for their opinions,
- Look at different countries based on how well they protect privacy, how well the courts keep an eye on things, and how easy it is to get help.
- Be open to scrutiny by Parliament or the courts.
- This will make it easier for data fiduciaries to plan ahead and make India more trustworthy in commerce and diplomacy with other countries.

8.2. Make sure that the Data Protection Authority is independent and responsible.

The Data Protection Board of India, which is now run by the executive branch, should be changed into an independent constitutional or statutory agency with:

- Fixed terms and job stability,
- Independence in enforcement and decision-making,
- Clear appointments and operations.

This would be in line with the best practices throughout the world and the Puttaswamy directive, which would strengthen institutional trust and rights-based enforcement.[41]

8.3. Set clear rules for contracts and transfers across countries

The government should let people know about model contractual terms, binding corporate rules (BCRs), and sectoral guidelines for legal cross-border transfers. This should have:

- Clear responsibilities for data processors and fiduciaries,
- Mandatory impact evaluations for transfers to countries with a high risk,
- Need for data principal notification and audit trails.

These kinds of technologies may help with compliance, make things clearer, and meet the demands of certain industries.

[41] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, at para. 180–183

ISSN: 2582-6433

8.4. Bring back Classification of Sensitive and Critical Data

India should rethink the idea of "critical personal data" by taking into account comments from different sectors and using a risk-based categorisation system. Possible groups:

- Critical data (defence, intelligence): Localised with stringent access constraints;
- Sensitive data (health, biometrics): transmission with extra security measures;
- General personal data: Transferable with permission and adequacy.
- This risk-tiered method will find a balance between national security and global interoperability.

8.5. Promote international cooperation and data diplomacy

India should be involved in both bilateral and multinational talks to encourage the flow of data across borders based on trust and respect. Important stages are:

- Joining or agreeing with the APEC Cross-Border Privacy Rules (CBPR) scheme,
- Working on mutual adequacy with the EU, UK, and important digital trade partners,
- Digital Economy Agreements (DEAs) let people share data more easily. This kind of diplomacy is very important for making sure that India becomes a member of the global data economy and networks of trustworthy partners.

8.6. Improve cybersecurity and ways to enforce the law across borders

India must do the following to protect transmitted data:

- Update its cybersecurity infrastructure and push businesses to use global standards like ISO/IEC 27001.
- Update MLATs and Data Transfer Agreements to make it easier to investigate across borders.
- Work with CERTs (Computer Emergency Response Teams) all across the world. This will lower the chances of cyber spying, data breaches, and digital crime across borders.

8.7. Increase public awareness and the ability of institutions

The government and civic society need to put money into:

- Digital literacy initiatives that teach people about data rights and consent,
- Helping small and medium-sized businesses deal with compliance expenditures,
- Paying for university research and new legal-tech ideas around privacy, AI, and data

ISSN: 2582-6433

ethics.

For any data governance system to work, individuals need to be well-informed and institutions need to be able to do their jobs.

Final Thoughts

India's journey towards a strong framework for cross-border data transmission depends on making sure that its regulatory policy is in line with constitutional ideals, economic pragmatism, and best practices from across the world. By developing institutions that are open and honest, supporting rights-based governance, and forming smart global relationships, India can become a digital power with trust at its heart.

Conclusion

The regulation of cross-border data flows in India is at a pivotal point, reconciling national interests, global commercial necessities, and individual privacy rights. The Digital Personal Data Protection Act, 2023 is a big step towards making data protection rules official. However, this framework's efficiency relies on more than just the lawmakers' intentions. It also depends on the strength of the institutions, the clarity of the rules, and the public's confidence.

India's legal system has to change from one where states have a lot of power to one where data is governed in a clear, responsible, and rights-based way. To be a trusted participant in the global digital economy, it also has to make sure that its own policies are in line with international data protection standards like the GDPR, APEC CBPR, and new guidelines on Data Free Flow with Trust (DFFT).

There are still some big problems that need to be addressed, such as executive overreach, enforcement limits, and a lack of defined sufficiency standards. However, a clear policy roadmap may help with these. This includes:

- Making independent institutions,
- Improving the power of the courts,
- Taking part in strategic data diplomacy,
- Improving the security of computer systems, and
- Raising public awareness.

ISSN: 2582-6433

The way ahead is to understand that data is not simply a resource, but a basic right that has big effects on democracy, development, and working together throughout the world. A balanced, future-ready strategy to cross-border data flow will help India safeguard its people, boost its economy, and show the world that it is a digital leader based on trust, openness, and technical brilliance.