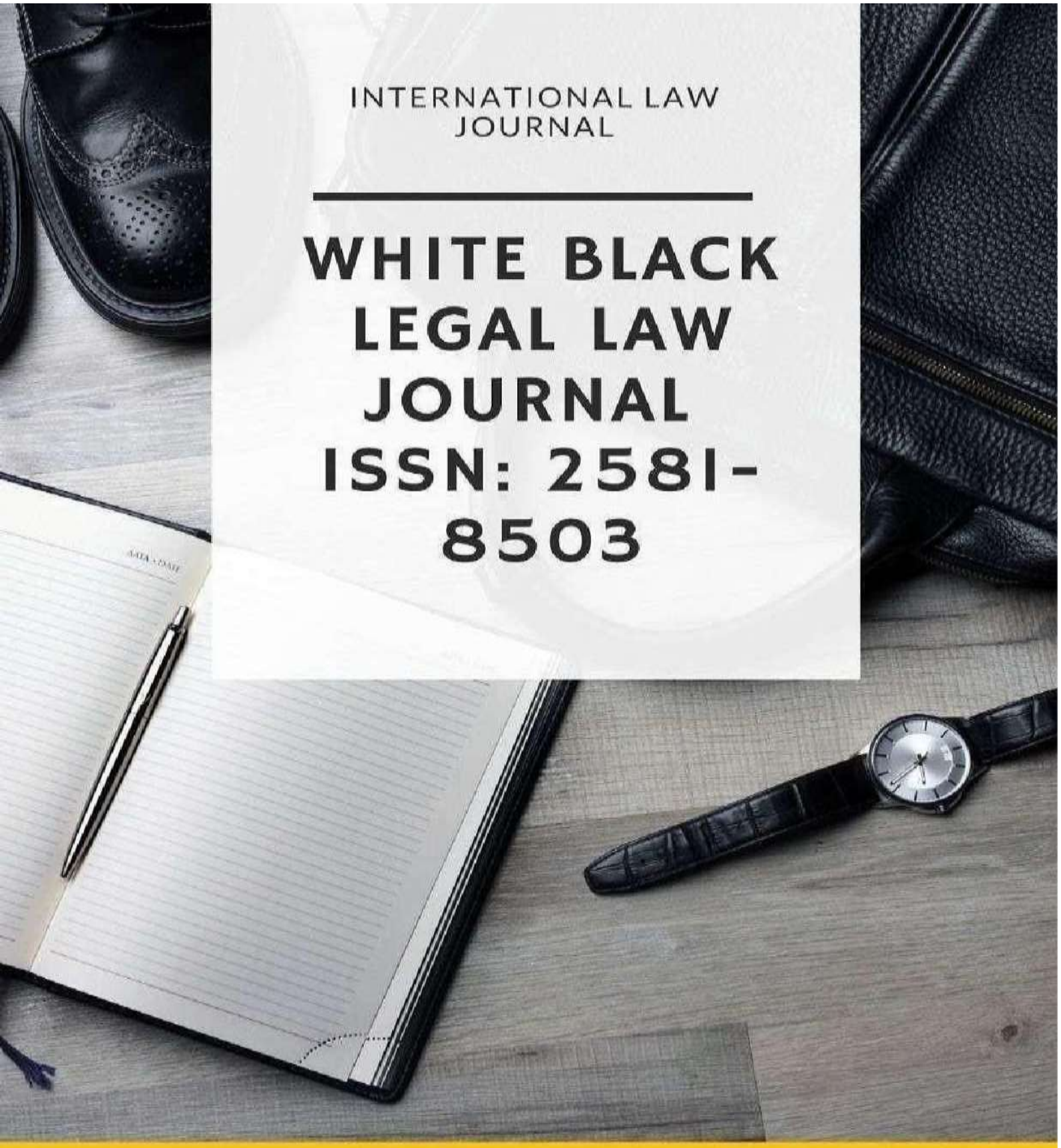

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

CROSS-BORDER DATA TRANSFERS: PRIVACY RISKS AND LEGAL IMPLICATIONS

AUTHORED BY - MR. PURANJAY DAS & MS. BASAVDUTTA KAR
Assistant Professor, Department of Law, Fakir Mohan University, Balasore, Odisha

Abstract

Despite the importance of cross-border data transfers, they can be very challenging to manage due to the privacy and legal risks associated with them. This paper aims to provide a comprehensive analysis of the regulatory landscape and the various legal frameworks that are designed to address these issues. The study explores various legislation, including the GDPR, the CCPA, and the PIPL in China. It also highlights the influence of notable legal cases, such as the Schrems II case, on data governance around the world. It proposes recommendations to help organizations balance the interests of their customers and the protection of their data with international legal obligations.

Keywords- Cross-border data transfers, Data protection laws, General Data Protection Regulation (GDPR), Data fiduciary, Data principal, Adequacy decision, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), , Negative list countries, Extraterritorial application, Data sovereignty, Data localization laws, Jurisdictional conflict, International legal cooperation, Data privacy regulations, Digital Personal Data Protection Act, 2023 (DPDP Act),

1. Introduction

Cross-border data flow is becoming more critical in today's interconnected internet economy. Global companies such as Facebook, Google, and Amazon move vast amounts of commercial and personal data across multiple countries. The collection and use of personal information around the world raises various issues related to security, privacy, and legal accountability. There are varying standards in different countries for protecting this data. Some of these include the exposure of individuals to surveillance and the misuse of it.

Cross-border data transfers are a complex issue that involves human rights, technology, and law. They allow businesses to deliver essential services and cross-border transactions, but they

can also conflict with national legislation aimed at protecting the privacy of individuals. Several new laws in different countries, such as China, India, and Brazil, have been enacted to restrict the export of personal information. These regulations aim to protect the privacy of individuals as data flows across different national boundaries. The legal rulings by the CJEU and the ECJ, such as the Schrems case, have highlighted the shortcomings of the current tools used to protect the rights of individuals.

The goal of this study is to examine the privacy consequences of shifting the territorial boundaries of data. It also looks into the implications of moving data across different jurisdictions with varying levels of protection. The goal of this study is to analyze the various legal principles and regulations that govern the global data governance process. It aims to find out if they can help resolve the issues related to the protection of personal information and economic integration.

The digital age has created a vital link in global communication and trade. The exchange of personal information has become a central component of global commerce and governance. Governments, businesses, and individuals rely on this data to conduct their operations, use AI, and make financial transactions. Unfortunately, the privacy risks and legal issues associated with this type of cross-border data transfer can be very different in different countries.

The regulation of cross-border data flows is complex and constantly changing. Some of the laws that restrict the ways in which personal information can be transferred include the European Union's GDPR, the CCPA in the US, and China's PIPL.

2. Privacy Risks in Cross-Border Data Transfers

a. Due to the varying regulations in different countries, it can be hard to comply with the privacy and data protection laws.

It is also very common for companies to encounter issues when it comes to complying with the privacy and security laws in different countries. Because of this, it is very important that they thoroughly understand the regulations in each country, especially when it comes to international business. This is especially important due to the rise of global connectivity and the increasing number of regulations in the digital age. It is now more important than ever that companies thoroughly understand the regulations in each country. Doing so can

help them avoid potential legal issues and operational problems. To ensure that they are following the latest regulations, businesses need to constantly monitor and adjust to the changes in the legal environment in different countries.[1]

b. Some countries have requirements for the localization of data. This involves storing certain types of information in their borders.

Countries have regulations that require certain types of data to be stored on servers within their borders. These regulations are usually focused on protecting the privacy and confidentiality of citizens' information and ensuring that the state has the necessary control over it. Despite the national security implications of data localisation, critics say it could hinder the flow of data across borders and increase costs for businesses. This is why it is important that organizations that operate in multiple jurisdictions have the necessary resources and skills to meet these requirements.[2]

c. Transparency and consent are the key components of ensuring that the users have the proper say in international data transfers.

When personal information is transferred overseas, users have to be aware of what their options are regarding the use of their data. This is because, if they are not informed about what their data is being used for, they might not be able to make informed decisions. Transparency and consent are also important when it comes to protecting the privacy of our users. The European Union's General Data Protection Regulation (GDPR) requires companies to follow a legal basis for the transfer of personal information outside of the country. This is because people have the right to know what their private information is being used for. However, if the users are not informed about what is being used and the legal consequences of the transfer, then it can prevent the data from being legally processed.[3]

---

[1] International Association of Privacy Professionals. (2023). Global privacy legislation tracker. https://iapp.org/resources/article/global-privacy-legislation-tracker/

[2] Kuner, C., Svantesson, D. J. B., Greenleaf, G., Bygrave, L. A., & Cate, F. H. (2017). Data localization and the free flow of data: A global overview. Journal of Law and Economic Regulation, 10(1), 1–29. https://doi.org/10.2139/ssrn.3437814
Data localization vs. the global Internet. Center for Democracy & Technology. https://cdt.org/insights/breaking-the-web-data-localization-vs-the-global-internet/

[3] Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
European Commission. (2024). International data transfers. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/international-data-transfers_en

d. Necessary safeguards must be implemented to protect data during its storage and transfer.

This applies to the storage and transmission of personal information, particularly when it is transported internationally. When this information is placed on a foreign server, it becomes more vulnerable to hacking, improper use, or illicit access. This can also occur when the receiving country has weak privacy laws. These include implementing strong encryption, VPNS, access controls, and security audits. In addition, the law, such as the General Data Protection Regulation (GDPR), requires organizations to have in place procedures that aim to ensure the security of their data. These procedures help organizations maintain the integrity and confidentiality of their data. They also help meet the legal requirements related to its security.[4]

e. Data breach notification: Complying with multiple jurisdictions' reporting requirements-

To comply with the reporting obligations of various jurisdictions, organizations need to notify the data protection authorities about a data breach. A data breach notification is an important process that organizations need to follow when it comes to protecting their customers' personal information. However, it can be very challenging to meet these obligations due to the varying legal requirements in different jurisdictions. The European Union's General Data Protection Regulation (GDPR) requires data controllers to notify the relevant authorities about a data violation within 72 hours. However, in the U.S., state laws have different timing and requirements for notification. Some countries only require notification to be made to victims if there's a substantial risk of harm. Others require it in cases of almost any breach. To meet these requirements, organizations need to have an effective incident response plan and assess their legal position in each jurisdiction.[5]

f. The regulation of data gathering and dissemination involves determining which regulatory bodies have the power to oversee it.

The regulation of data protection covers the powers of governmental agencies or groups to enforce privacy laws and oversee the practices of data processors. Jurisdiction can be affected by how the personal information is handled by multinational corporations or transferred across international borders. This is especially true when there are overlapping

4 European Commission. (2024). Data protection: Security of personal data. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-general-data-protection-regulation-gdpr-govern_en

5 IAPP. (2023). U.S. state privacy legislation tracker. International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

and competing laws in different countries. For instance, under the GDPR, the lead supervisory authority for the data controller will be in the country where the main establishment is located. Due to the varying regulations in different countries, it is important that organizations carefully consider the legal jurisdiction and data flows in each region when it comes to regulating their operations. This will help them ensure that they are following the latest laws.[6]

g. International agreements cover the management of data transfers between nations. It involves navigating through treaties and frameworks designed to govern such transfers.

The establishment of treaties plays a vital role in facilitating the exchange of information between different countries, especially when privacy laws vary globally. These mechanisms and agreements aim to establish a level of trust and uniformity in the transmission of data. One of the most common examples is the EU-US Privacy Shield. This framework allows U.S. businesses to receive personal information from the EU in compliance with the General Data Protection Regulation (GDPR).[7] The Convention 108+ of the Council of Europe provides for the protection of cross-border data. However, these agreements are complex and can be prone to change due to legal challenges. To avoid getting banned, organizations should regularly monitor the content and existence of these frameworks.[8]

h. Addressing the requests for information made by the government in different jurisdictions is a key priority for law enforcers.

Due to the complexity of the situation, it is often difficult for companies to comply with the requests made by law enforcers. While protecting the privacy of their users, they also have to respond to the government's demands. The legal boundaries and procedures governing the access of personal data in different countries vary depending on national security directives and court orders. For instance, the US can use laws such as the CLOUD Act to force companies to turn over international data stored in the country. However, the General

[6] European Commission. (2024). One-stop-shop mechanism. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/one-stop-shop_en
European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[7] European Commission. (2023). EU-U.S. Data Privacy Framework. https://commission.europa.eu/document/fae2a6c1-9cb8-4571-8b7e-e2ebcf1a97db_en

[8] Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). https://www.coe.int/en/web/data-protection/convention108-plus

Data Protection Regulation (GDPR) prohibits the disclosure of such information unless it's related to EU or national laws. The legal frictions that result from the requests made by law enforcers have a significant impact on the privacy and confidence of users. It is therefore important that companies take the necessary steps to balance their responsibilities with the needs of their users.[9]

i. Data retention and deletion: Managing conflicting requirements for data storage duration and disposal.

The concept of data retention and disposal is complex, especially when dealing with the handling of personal information that's collected across different borders. Some countries have strict minimum periods for the retention of certain types of data, while others allow the destruction of those that are no longer required for the purposes that they were collected. In certain countries, such as India and the US, laws may require longer retention periods. This can result in organizations having to develop policies that are specific to the requirements of the law, which can be costly and can lead to the failure of the organization to comply. Another issue that can arise is the lack of consistency in the implementation of policies. Having the right data management policies can help prevent unauthorized access and use of data. Failure to keep these responsibilities in order can lead to various issues, such as non-compliance and legal penalties.[10]

j. Transnational litigation involves the collection and handling of evidence and e-discovery in different jurisdictions.

Due to the complexity of cross-border litigation, it can be very challenging for businesses to comply with the laws in different jurisdictions. For instance, in some cases, a party may be required to reveal information that is protected by privacy laws in another country. Due to the complexity of the e-discovery process, it can be hard to determine which of the various steps should be taken to protect the privacy of individuals. For instance, in the U.S. courts, they can require broad data disclosures, while the EU's General Data Protection Regulation (GDPR) imposes strict restrictions on the transfer of personal data to third

[9] U.S. Congress. (2018). Clarifying Lawful Overseas Use of Data (CLOUD) Act. H.R.4943 – 115th Congress (2017–2018). https://www.congress.gov/bill/115th-congress/house-bill/4943
European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
[10] U.S. Department of Health & Human Services. (2013). Health Insurance Portability and Accountability Act of 1996 (HIPAA): Security and privacy rules. https://www.hhs.gov/hipaa/index.html

parties. To minimize the complexity of cross-border litigation, organizations can use various strategies to manage their risks. These include implementing legal assistance treaties, establishing data transfer agreements, and redacting and anonymizing information.[11]

3. Legal Frameworks Governing Cross-Border Data Transfers

Due to the existence of various regulations and laws, the information flow across international borders is affected by a variety of factors. The latest example of this is the Digital Personal Data Protection Act of 2023. This Act aims to protect the privacy of individuals.

a. Digital Personal Data Protection Act, 2023 (DPDP Act)

The Data Protection Act of India is a national legislation that is modeled on international standards such as the GDPR of the European Union.

Government-Controlled Cross-Border Transfer System

The Data Protection and Data Protection Act (DPDP) allows cross-border transfer of personal data. However, it also allows the government to restrict or prevent the transfer of data to certain countries. This is because India's government has the power to prevent the data from going to countries that do not have strong privacy laws. For various reasons, such as national security, the government can restrict the flow of data to certain countries.[12]

Consent-Based Data Processing

The information that users provide must be specific and explicit in order to be able to understand how it is being used. This is done through the consent process, which should be clear and explicit. Users should also be aware of the other details about their data being shared. If a data principal revokes their consent, the information processor must stop processing their data. This ensures that people have the ability to see how their data is being used.[13]

Accountability of Data Fiduciaries

Even if a third-party processor is operating outside of India, the data fiduciaries who oversee the processing of data have to ensure that the protection of their customers' information is upheld. Responsible processing of personal data can help improve people's behavior. It can

[11] The Sedona Conference. (2011). International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Legal Proceedings. https://thesedonaconference.org/download-pub/81

[12] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023

[13] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023

also protect their privacy and prevent them from being exposed to harmful effects.[14]

Data Protection Board of India (DPBI)

A regulatory authority is established to resolve disputes involving the transfer of international data. It can impose penalties, direct corrections, and investigate violations. A formal process is also used to punish those who fail to handle such data properly.[15]

Prohibition of Transfer to Restricted Countries

Following the law's stipulation that transit is generally allowed, there is an explicit fallback provision that allows the government to prevent all transfers within a country or region if it is unsafe. This system is similar to what other jurisdictions have used.[16]

b. Information Technology (IT) Act, 2000 – Section 43A & IT Rules 2011

Accountability for Data Breach (Section 43A of IT Act)-

According to Section 43A of the IT Act, a corporate body is liable for damages caused by a data breach if it has negligently handled sensitive information. Even if the information is transferred outside India, the company still has to pay the damages.

Protection: When it comes to handling personal information, companies are liable for any damages that arise due to the improper use.[17]

Consent for Data Transfer (Rule 7 of SPDI Rules)-

The personal data of the recipient may be transferred to another country or entity

- if the consent has been obtained and the person has agreed to the transfer
- The recipient is bound by the same data protection standards as Indian law.

Protection: This prevents the data from being forwarded to companies or countries that do not offer the same level of privacy protection.

Definition of Sensitive Personal Data (SPDI)

The concept of sensitive personal data (SPDI) refers to the information that a person has on themselves, such as financial information, health data, and passwords. These are protected by strict rules under SPDI.

Protection: risk categories of data are protected from unauthorized access and use. This

[14] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[15] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[16] European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[17] Government of India. (2000). The Information Technology Act, 2000 (No. 21, Acts of Parliament, 2000), Section 43A. Ministry of Law and Justice. https://www.indiacode.nic.in/handle/123456789/1999

ensures that you'll have the most privacy-friendly experience when sending data overseas.[18]

Reasonable Security Practices (Rule 8 of SPDI Rules)

An organization must have a security program in place to protect its data at rest and in transit.

Protection: The use of domestic and international standards ensures that sensitive information is protected when traveling across international borders.

International Commitments & Future Outlook:

i. Bilateral and Multilateral Data Transfer Agreements-

In addition to the usual framework agreements, India is also expected to seek multilateral or bilateral agreements that provide for the recognition of a "deemed equivalent" status for the information collected by different countries.

- The protection of personal information is a fundamental aspect of the relationship between India and other countries.
- The goal of an agreement is to provide a reliable and secure flow of information between India and various trading partners, such as the US, EU, and ASEAN.
- Academic writers also raise concerns about the lack of clarity regarding the law and the legal basis for cross-border companies.[19]

ii. Interoperability with Other Jurisdictions-

The DPDP Act of India provides for interoperability and flexibility with international regulations, such as the CCPA of California or the EU's General Data Protection Regulation.

- The Act does not prevent the transfer of international data. It only blacklists countries that are not trustworthy.
- The Act provides India with the opportunity to establish reciprocity agreements with other privacy regulations.

Protection: Interoperability reduces legal obstacles and helps ensure that the privacy of the data is protected.[20]

[18] Government of India. (2011). Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Ministry of Electronics and Information Technology. https://meity.gov.in/writereaddata/files/GSR313E_10511(1).pdf

[19] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[20] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-Act-2023

4. Policy Recommendations and Future Directions

India's data protection system has made significant progress under the Digital Personal Data Protection Act, 2023 (DPDP Act). However, regarding cross-border data transfers, the Act has several loopholes and ambiguities that may raise concerns for global stakeholders.

a. Loopholes in the DPDP Act, 2023 – Cross-Border Data Transfers

1. *Lack of Adequacy or Risk-Based Assessment-*

Unlike the EU's GDPR, which only permits data transfers to nations with sufficient levels of protection, the DPDP Act:

- Allows transfers to any country by default,
- Unless the Central Government notifies a "negative list" of restricted countries (Section 16).

Issue: There is no official procedure to assess whether beneficiary nations offer an equal or adequate degree of data protection.

Suggestions: In order to address this gap in the adequacy and risk-based assessment in the DPDP Act, 2023, it is suggested that the Act may be amended to integrate the formality of the adequacy evaluation framework for the cross-border data transfer. This framework should mandate that the Central Government, after consultation with the Data Protection Board of India, evaluate the adequacy of data protection in recipient countries according to clear, objective filters— such as the existence of a comprehensive data protection law, enforcement, rights of individuals, and availability of grievance redress. Instead of just following a negative list to make the adequacy determination, India could consider having a "positive list" model like the European Union's GDPR, where transfers are only allowed to countries that have been declared inadequate and may get the adequate status. What's more, even for non-listed countries, transfers could still take place under other transfer instruments, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). Adversely, if it is to implement such a scheme, it would bring Indian in line with international best practices, increase legal certainty for businesses, and provide more robust standards for privacy protection for individuals.[21]

2. *No Differentiation of Data Sensitivity-*

The law treats all personal data uniformly during transfer—there is no distinction between:

[21] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-act-2023

- General personal data,
- Sensitive personal data (like health, biometric, or financial data)
- Critical personal data.

Issue: Transfers of high-risk or sensitive data to countries with weak protections are not subject to extra scrutiny.

Suggestions: To mitigate against the lack of differentiation for degrees of data sensitivity in the DPDP Act, 2023, the law should be revised to enable risk-based categorisation of personal data, particularly in the case of cross-border flows. They should classify data as general, sensitive, and critical personal and prescribe the required level of protection and the nature of the transfer. It should be a matter of course that where the data being transferred is particularly sensitive -- biometric, financial or health data - far stricter safeguards be put in place, such as mandatory encryption, advance approval by a regulatory authority or transfer only to jurisdictions with sufficient data protection rules. For sensitive personal data, the government could mandate that it be kept and processed by India or its agencies or highly supervised circumstances. The Act would improve risks of misuse or unauthorised access in foreign territories by imposing graded protection levels according to the data sensitivity, which would no doubt provide better protection for individual privacy and national data security.[22]

3. Limited Role of the Data Protection Board

The Data Protection Board of India (DPBI) is:

- An executive-appointed body, not fully independent,
- Given limited proactive enforcement powers over cross-border data misuse.

Issue: Individuals have no clear recourse if their data is mishandled after an international transfer.

Suggestions: In order to address the problem of the limited role of the DPBI, an amendment to the DPDP Acts, 2023, to strengthen the independence, powers and enforcement of the Board, especially in cross-border data misappropriation cases, should be made. 'There should be checks and balances in the way in which the members of the DPBI are appointed, involvement of judicial or parliamentary oversight to ensure institutional autonomy, and to minimise influence of the executive. The second is to grant the Board the power of proactive investigation, so that it can undertake investigations into cross-border data breaches without

[22] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. https://prsindia.org/billtrack/the-digital-personal-data-protection-Act-2023

having to rely on individual complaints in the first place. Third, the law must provide clear channels for individual redress, including when data is misused outside India, by permitting affected data principals to file complaints and being awarded redress. Second, the Board should be empowered to work together with foreign data protection authorities so that enforcement does not end at India's shores. Such empowerment of the D BPI would give substantive accountability and safeguards in a more and more interlinked digital network.

4. *No Clear Redress for Cross-Border Harms*

If an individual's data is misused by a foreign entity, the Act:

- Does not provide a clear mechanism for redress or enforcement outside India.
- Fiduciaries are responsible, but jurisdictional enforcement is unclear.

Issue: In case of a breach abroad, users may be left without remedy or compensation.

Suggestions: To make up for the lack of clear remedies for cross-border data harms that the DPDP Act, 2023, fails to address, the DPDP Act, 2023, should be revised to provide specific language regarding international legal cooperation and user compensation mechanisms. This could take the form of bilateral agreements or multilateral arrangements that would permit reciprocal recognition and enforcement of data protection laws between India and foreign jurisdictions, enabling India's Data Protection Board to work collaboratively with the regulatory authorities of other countries. Further, cross-border transfers by data fiduciaries should also make it obligatory to provide Indian data principals grievance redressal, appoint a local authority or agent to address any issues and to ensure continued compliance with the provisions of this Act. That way, if data were processed outside of the country, there are still enforceable avenues for users to try and achieve a remedy. Enforcement of such provisions would hold foreign data abusers directly accountable while offering recourse to people whose data privacy is violated beyond the shores of India."

5. Conclusion

Due to the increasing number of cross-border data transfers, it is important that the legal boundaries are set to address the privacy risks associated with these transactions. Although regulatory frameworks have been established to protect the privacy of individuals, technological advancements will determine how this information is protected in the future. This study aims to provide a comprehensive analysis of the various factors that affect the protection of individuals' data.

The rapid emergence and evolution of the digital economy has resulted in the need for cross-border data flows. However, these transactions can also expose individuals to various privacy and legal risks. Some of these include the loss of control over the data, state surveillance, and the lack of legal solutions.

Navigating the maze of international privacy laws can be challenging. From the European Union's General Data Protection Regulation (GDPR) to India's Digital Personal Data Protection Act (DPDP), it is important to plan for your company's compliance.

Despite the various provisions of the DPDP, the country-level responses in India still need to be developed. While the law provides for the establishment of principles such as data containment and minimisation, it does not address the enforcement of the regulations.

The balance between international and domestic data flows is dependent on various factors. Besides having strong national laws, the other factors that affect the flow of information include the availability of technical controls and the establishment of international agreements. For businesses, it is also important that they are able to secure informed consent and implement effective accountability measures. On the other hand, policymakers should focus on developing effective global co-operation agreements and putting the privacy rights of citizens at the center of their digital governance.