Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 3 (2025)

Data Privacy and Security in a Globalized Digital World: Legal Perspectives on Cross-Border Data Flows

Garima[1*]
[1]Research Scholar, School of Law, Sushant University, Gurugram, Haryana-122003, India
Dr. Shreya[2]
[2]Assistant Professor, School of Law, Sushant University, Gurugram, Haryana-122003, India

ABSTRACT
As information systems become a weapon for controlling the future, we are living in a time when they are becoming a new weapon of war. The flow of data across national borders is a vital resource for economic and informational development in any country. Cross-border data flows are increasingly important in international trade due to the frequent transfer of employee and customer data across borders. Using cross-border data exchange as a case study, this paper discusses its privacy implications. As neither the Digital Personal Data Protection Act of 2023 nor the Information Technology Act of 2000 provide any protection for cross-border data transfers, the report discusses a cross-border data protection policy. Particularly, the Digital Personal Data Protection Act, 2023, provides no information about how data can be transferred between countries or processed for data principals outside of the country. When some countries restrict data movement abroad by enacting laws concerning data localization, they negatively affect international trade and development. The question then arises: What types of data, and in what quantities, are nations required to restrict? Here is a comparison of the General Data Protection Regulation of the European Union, the Asia Pacific Economic Cooperation Privacy Rules, and the Privacy Shield Framework between the EU and US. To conclude, this paper suggests the need for uniform laws to protect cross-border data and their universal applicability.

Keywords: Cross-Border, Legal Perspective, Digital World, Data Privacy and Security

INTRODUCTION
Law and technology adaptation are not necessarily new concepts in the area of trade law[1]. Digital technologies are no different, as the WTO membership in 1998 recognized the deep impact of the Internet on all aspects of trade, as exemplified by the Work Programme on Electronic Commerce from 1998. IP protection and the rules governing trade in goods and services may need to be changed.

Nevertheless, a number of studies have examined the most urgent areas for such changes as well as the best ways to achieve them, taking into account their political feasibility. While technology at the time was still at level 2.0, policy and scholarship were both mobilized simultaneously due to the dual level of technology? As a platform to sell goods and services online, the Internet was viewed primarily as 'e-commerce' at first, but its potential as a general-purpose technology (GPT) was overlooked[2]. As trade conditions changed and global value chains (GVCs) emerged, these effects became palpable and were considered by subsequent studies. Yet, despite its importance to the economy and its profound implications for society, data remained largely ignored. Digitalization's disruptive properties and the impact of data have only recently been recognized as aspects of the Fourth Industrial Revolution. Policy and academic circles have recognized that a change in legal

design beyond simple adjustments is needed as Big Data and artificial intelligence (AI) emerge as distinct new phenomena. During these latter stages, a new relationship was discovered between digital trade and privacy protection, which was hotly contested. Trade law and privacy law haven't been connected in the past, and legal frameworks haven't addressed their interface. The impact of international economic law on non-economic interests has been vigorously debated in scholarly and policy circles, but privacy has rarely held a prominent place[3]. The growth of data value and Big Data analytics are defining a new field of competition. Many have referred to data as the 'new oil' in recent years, recognizing its importance to economic processes. There have been many studies demonstrating the vast potential of data, and the dependence of new and emerging technologies on data, such as artificial intelligence. Meanwhile, this increased dependence on data posed a new set of challenges. Researchers and policy-makers have both acknowledged that data collection, use, and re-use impact privacy. The EU General Data Protection Regulation (GDPR) is the best example of the data protection laws reform triggered by these challenges[4].

As illustrated later by a comparison of EU and US approaches to data protection, the reform initiatives are not based on society's understanding of constitutional values, citizen relationships with the state, and the role of the market. There is no coherence between them, and they are embedded in cultures and societies.

In addition to tensions over data, tensions over cyberspace sovereignty have also been re-ignited[5]. As data is intangible and ubiquitous, locating it is particularly difficult, since bits of data, even those related to one activity, might be located anywhere. Increasing data value and risks, as well as contentious jurisdictional issues, have forced governments to find new ways to assert control over data - in particular by prescribing various measures designed to keep data, its storage, or its suppliers within their jurisdiction by 'localizing' them. In addition, data barriers have serious repercussions for trade, causing a conflict between data protection and data sovereignty, as well as trade agreements that aim to boost trade, innovation, and growth. Generally, data's increasing role in society has increased the complexity and diversity of the interface between trade and privacy protection[6]. Regulators need to consider how their designs can strike a balance between the interests of national and international stakeholders, as well as economic and noneconomic considerations. As a result of this complex background, this study provides a more comprehensive understanding and contextualization of aspects of trade law related to data protection. Because of the proliferation of rules relating to the flow of data, this article examines the way free trade agreements (FTAs) are framing data protection and how reconciliation mechanisms are being developed to reunite trade and privacy. Analyses of domestic privacy law developments serve as the basis to examine whether trade law has intruded into domestic privacy law developments too rapidly and to a greater degree.

Statement of Problem

While the growth of the world economy, the phenomenon of cross border data has brought benefit and risk for business, especially on data protection. As the global sharing of data continues to rise, the private and public entities as well as citizens have become more cautious while sharing their information.

Currently, a significant number of countries do not succeed in enforcing their laws strongly, or they have different data privacy laws as others, and this makes a highly insecure environment for data, which might be intruded, exploited or get in touch with cyber threats and unauthorized persons[7]. Moreover, there are data localization laws as well as there are highly developed legal systems as in

the form of localized legal policies which have aimed at enabling cross-border data flows to protect privacy rights also, which in turn has made the international data regulation more complex. Unfortunately, despite these measures, we still lack insight into the effect that cross-border data transfer has on privacy and how current legal solutions regulate such a process. Through this study aimed at solving the following research problem; Analyzing cross-border data flows, privacy risks they pose and the adequacy of the prevailing laws that mitigate the problem.

Objective

As press reports suggest enormous volumes of cross-border data flows and the need to understand how they are affecting data privacy for such countries. This paper focuses on the impacts of digital information globalization which would include global commerce, innovation, and communication. In addition to the examination of these data flows the current work concerns privacy and data protection issues, security threats. Further, this research will look at how cross border data transfers are regulated and what laws and policies exist to monitor the flow of data across borders, and how privacy issues are addressed across the globe. In this study, author brings the two seemingly contradictory concepts of globalization of people and protection of personal data into equilibrium through this evaluation.

RESEARCH METHODOLOGY

This research uses a doctrinal legal research method to consider data privacy and security laws in relation to cross-border data transfers. You'll also explore primary sources of information such as statutes, regulations, court cases, and international agreements (e.g., the General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act of 2023) as well as peer-reviewed articles, working papers, and data-sharing protocols. Secondary sources are academic articles, data protection authorities' reports, and policy papers. For the sake of comparison, similarities and differences with respect to the European Union, USA and India are pointed out. This method allows us to critically manage the delivery of legal challenges and voids which govern the transnational movement of data. The study also conducts the legal sufficiency, data localization mandates and digital trade impact analysis & provides an integrated image of the changing worldwide data governance environment. The method of the content analysis is an instrument for analysing and reconstructing legal materials.

Regulations on privacy protection at the global level

Therefore the legal systems, social culture together with the relative economic sentiments within the nations in one global study the authors unveiled that the experimentation in data privacy regulations is different from others[8]. These approaches aim to protect people's data privately while feeding the serving organizations. governments, as well as world trade as well. Due to the fact that data is on the fast rise when it crosses the national borders through and through the use of digital platforms, cloud and e-commerce the regulation of data privacy has established themselves as the main nexus of security vs privacy in the dynamic new digitized, globalised world.

It is widely recognized that the GDPR, which is approved by the European Union, is the most comprehensive regulatory framework for data[9]. It was enacted in 2016, and it has been used as a benchmark when it comes to providing privacy regulations on the international scene. Considering it is made up of seven principles including; Data Minimization whereby only sufficient data ought to be processed from the individual for the intended legal purpose and Lawfulness whereby data can only be processed with consent from the user. Among the rights granted by the GDPR are the right to access data, the right to erasure, and the right to data portability, which allows users to move data

between service providers. A level of privacy protection adequate to protect EU personal data cannot be exported outside the EU without adequate safeguards, according to the expert[10]. When it comes to the transfer of data across borders, there are a lot of rules. A high level of data protection is ensured through measures such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), which guarantee that even data transferred cross-organizationally is protected.

The United States, however, uses a sectoral approach to data privacy, which means that different laws apply to different sectors rather than having a single legislation. Information pertaining to health insurance is protected under HIPAA, while information relating to children under 13 is protected under the Children's Online Privacy Protection Act (COPPA)[11]. Consumers' financial information must be protected by financial institutions, and the GLBA governs this. In June 2018, California passed the California Consumer Privacy Act (CCPA), which in many ways mirrors the GDPR, and while the United States does not have a federal data protection law. There are three rights provided by the CCPA for California residents: the right to know, the right to delete, and the right to opt out[12]. While there is no national privacy law, the regulatory framework has developed state- and sector-specific complexity, provoking discussions on the federal privacy law.

A number of countries such as China, Russia, and India insist on data localisation and data sovereignty which regulates those particular categories of data, primarily sensitive or crucial data, has to be processed and stored locally within the country. This approach is mainly informed by national security, economic nationalism and more government control on data flows. For instance, China's Personal Information Protection Law (PIPL) and its Cybersecurity Law require critical infrastructure data withhold within the country and limit overseas transfer of personal information[13]. Same as that, the Data Localization Law in Russia, which obligates foreign companies that gather information about Russian users, to store it in Russia, strengthens state Regulation of the Internet and digital data. The newly passed Digital Personal Data Protection Act, 2023 in India barred transfer of sensitive personal data to other countries and insists on localization of some data due to national security and economic reasons[14].

Australia has embraced both co-regulation and self-regulation while Japan operates self-regulation with both having government intervention with an emphasis on compliance. At the moment, Australian legislation that regulates the processing of personal information is the Privacy Act 1988; however, various industries can establish their codes of practice as long as they do not contradict the general legislation[15]. The final example of flexible legislation is the Act on the Protection of Personal Information in Japan (APPI) that permits prescriptive and mandatory-industry standards and voluntary compliance but has a high level of data protection principles[16]. A similar example is GDPR where Japan became the first country outside EU to gain adequacy decisions, further helping simplify the cross border data transfers and encouraging data protection.

In the Asia-Pacific territory, the APEC Cross-Border Privacy Rules (CBPR) system is a semi-binding, regional system aimed at ensuring privacy and promoting cross-border data transfer[17]. Companies that have certification have particular privacy, and the system maintains sharing of data between APEC member economies, thus enhancing confidence in trade within the digital market.

The theoretical literature on data protection has identified that some countries, including Brazil and South Africa are in the 'middle' position in terms of data protection and privacy. As Berwanger et al, (2019) observe the Brazilian LGPD is a General Data Protection Law based on the GDPR, but

unique in its applicability to both public and private sectors[18]. South Africa's POPIA also is based on international norms and standards but reflect the context of the South African socio-economic environment.
Multilateral treaties and trade related relationships are also influencing the world's privacy norms. For instance, the USMCA agreement has a clause that allows Cross Border Data Flows while at the same time preserving the privacy of data[19]. The EU through adequacy decisions accredits third countries with similar data protection regimes so as to enable the transfer of data to such countries such as Japan, Switzerland and Israel among others.
There have been ongoing attempts to standardize the framework of data privacy across the world; however, the world is yet to gain a common model and importance on the issue. In the future, new privacy regulations will be required when new technologies like artificial intelligence, big data and IoT arrive. The issue for policy makers is to strike the right balance within data protection, on the one hand, and, on the other, innovation especially in the context of the emerging digital economy.

Data flows across borders in the era of digitization: a new role for cross-border flows
Internet networks are networks of networks, so data must be transferred between them in order for the Internet to function. When data packets are transmitted over the internet, they may pass through several countries before reaching their final destination, so it is sometimes difficult to determine where a particular data flow originated[20]. Approximately 11,500 institutions, 4 billion accounts, and 44.8 billion accounts use SWIFT to send financial communications to more than 200 countries every day[21]. It is becoming increasingly important for the digital economy to grow in the twenty-first century because free exchange of information is a great value in the digital economy. The Internet can now be accessed via devices other than computers and smartphones. In addition to shoes, televisions, printers, automobiles, motors, and household appliances (refrigerators and coffee makers), devices can now be connected to the Internet. Communication between devices connected to the Internet of Things (IoT) is handled by built-in applications. Businesses, governments, and individuals can benefit from the Internet of Things (IoT) by improving income, productivity, and reducing expenses. Digital environments today raise cross-border data privacy concerns because they use different networks and devices to share information.

The number of social media users worldwide is projected to reach 4.261 billion by 2021, according to Statistics[22]. Social networking companies are competing to disclose more personal information about their users based on this data. Increasingly interconnected virtual worlds pose a significant privacy risk for international data transmission. Our law requires companies to safeguard users' personal information and to comply with privacy requirements. A data protection program protects personal information from loss, corruption, and tampering. There is a significant difference between "data protection" and "data privacy," despite the fact that they are sometimes used interchangeably. The definition of data privacy specifies who is permitted to access the data, whereas the definition of data protection specifies how it can be actively accessed. Human rights are universally recognized and must be protected by all states, including the right to privacy[23].

As data (and 'big data' in particular) become more valuable, sharing data across borders has greater benefits. Throughout the 21st century, it has been regarded as a defining characteristic of

globalization as a connection between the global economy and the global community. Innovators use international data transfers to facilitate technological advancements and scientific advancements. Across great distances, remote working and remote learning tools are essential for employees, engineers, technicians, and students in this era of social distancing.

Google has grown into one of the world's most profitable companies despite only being thirteen years old. Its immense data storage, which includes Gmail users' data, documents, and photos, has contributed to Google's success. Due to the lower costs involved in data encoding, storage, and distribution, transborder data transfers reduce transaction and trade-related costs. A new study shows that Internet usage reduces trade costs by 26% using data from the United States International Trade Commission.

Privacy and security challenges of Cross Border Data Flows

International data transfers are required for business and economic growth today, which involves digital data moving across borders. Concerning privacy and security issues though, they prove to be rather enormous obstacles[24]. The latter is not unconnected with the fact that various countries have dissimilar and sometimes inadequate data protection legislation. GDPR in the European Union is an example of strict regulations enforced in this area, while it is quite the opposite in other nations, with their standards being quite lenient leaving personal information vulnerable when transferred[25]. Besides this, human beings with low privacy rights have their privacy infringed by other governments within countries that do not guard privacy.

When data moves across various networks and servers, some of which may not have adequate security measures to lock out an attack, flowing data across borders also enhances the risk of cyber-attack[26]. It is even more amplified by the fact that organizations hire third-party service providers including cloud storage and another problem when there is a breach or misuse of data is the hardest time to make organizations answerable because of complications of jurisdictions. In response, many countries have passed data localization laws that mandate that their citizens' data be stored within their borders despite the realization that such actions commonly slow innovation around the world and increase operational expenses. CCPA and GDPR are also regulatory frameworks that differ across the border and are the issues that complicate things for companies[27]. Nonetheless, the issues prevailing in cross border information flows are fundamental for modern technologies, including artificial intelligence and cloud computing. Security measures such as data privacy agreements, encryption and minimization have to be recognized and adopted internationally because security, privacy of data and benefit of sharing data is global.

A case involving the right to privacy of individuals in India was heard by Justice K.S. Puttaswamy (Retired) and others v.s Union of India and Others. According to the Supreme Court, this right also extends to internet privacy, which is a constitutional right recognized by the Constitution. Taking this case into account, the Court continues to affirm that Article 21 protects the right to privacy as a fundamental freedom. Data protection laws offer limited protection to sensitive personal information, but there are no comprehensive laws protecting cross-border data.

Indian Legal Framework

India has a sector-specific approach to data protection that is complex and comprehensive. The data protection law in India is different from those in other countries; it combines statutes, rules, and guidelines to protect personal information. Most of the provisions of the Information Technology Act, 2000[28], were amended by the Information Technology Amendment Act, 2008[29]. Section 43A concerns 'reasonable security practices and procedures', while the Information Technology (Responsible Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 address 'reasonable security practices and procedures'[30].

However, these regulations have a limited scope and coverage: most of their provisions only apply to sensitive personal information, and corporations automating data processing cannot enforce them, and only a limited number of consumers can take action to enforce them. A comprehensive privacy law has been under consideration in India for some time in order to address these limitations. There is no information about how far the draft Right to Privacy Law 2014 has progressed, but it is under consideration by the Government. There are no central, national bodies or complaint mechanisms that regulate data protection in India at this time. Currently, the Data Protection Authority of India (DPA) is being considered as part of the draft Right to Privacy Law. Offshore transfers of sensitive data are subject to some very limited regulations. Only countries with reasonable security practices and procedures are allowed to receive sensitive personal data or information under the Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011. There are a number of sensitive information types covered by the 2011 rules, including passwords, financial information, health information, sexual orientation information, medical records, and biometric information.

International Conventions

Cross-border data transfers are currently governed by three mechanisms: the European Union's General Data Protection Regulations (GDPR), the Privacy Shield Framework between the EU and the U.S., and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (APEC)[31].

1. In December 2013, the General Assembly passed resolution 68/167 concerning surveillance and interception of communications, which is detrimental to human rights[32]. During its resolution, the General Assembly reaffirmed that online privacy is just as important as offline privacy, and requested that all countries uphold and defend this right. Among other things, all countries must review their communication data collection procedures, practices, and legislation. It is the responsibility of States to comply fully and effectively with their international human rights obligations.

Whenever a civil individual's privacy rights have been violated, their privacy rights must be assessed according to international human rights standards. According to the International Covenant on Civil and Political Rights, which has been ratified by 167 countries at the moment, an individual's right to privacy, their family, their home, their correspondence, as well as their honor and reputation cannot be interfered with or attacked arbitrarily or unlawfully[33]. It added that all individuals under the law must be protected against such interferences and attacks. International human rights treaties do not differ from this document in terms of the rights and freedoms they stipulate. There is no “privacy” human right but there is a right to privacy which can be violated in

the paramount interest of necessity, legitimacy and proportionality. During 2014, the High Commissioner for Human Rights published the report on the right to privacy in the digital age (A/HRC/27/37) recommending a study on the issue[34]. The right to privacy is violated arbitrarily or unlawfully in several States because of weak legislation and enforcement, weak procedural safeguards, and ineffective oversight, which contribute to a lack of accountability for those violating the right. UN Human Rights Council experts are known as Special Rapporteurs. Their tasks include studying and reporting on specific issues, such as privacy rights. As the first Special Rapporteur on privacy, Professor Joseph Cannataci (of Malta) was appointed by the Human Rights Council in July 2015[35]. Three years are the terms of the appointment. It is the responsibility of the Special Rapporteur, pursuant to Resolution 28/16 of the Human Rights Council, to gather relevant information, including international and national frameworks, national practices, and experiences, and to make recommendations relating to privacy promotion and protection, including technological challenges, in light of trends, developments, and challenges related to them. A number of stakeholders or parties interested in human rights provide the organization with information on human rights, including states, the United Nations, its agencies, programs, and funds, regional human rights mechanisms, national human rights institutions, civil society organizations, companies, and others.

Make recommendations and proposals to the Human Rights Council, including those related to the digital age, regarding best practices and principles that may hinder the promotion and protection of the right to privacy on a national, regional, and international scale. Promote an integrated and systematic approach to topics relevant to the mandate by participating in and organizing relevant international conferences and events. It is crucial that the right to privacy is promoted and protected, taking into account the particular challenges associated with the digital age, and that effective remedies are provided to those whose rights have been violated in accordance with international human rights law. Gender considerations should be incorporated into the work of the mandate. Unless there is a credible claim to the contrary, report any apparent violation of the right to privacy, wherever it occurs, in accordance with article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights[36]. The Council should be aware of challenges arising from new technologies as well as situations of concern to the Council and the UN High Commissioner for Human Rights. The Human Rights Council and the General Assembly should receive an annual human rights report. To the Human Rights Council, the Special Rapporteur submitted a report titled A/HRC/31/64 in March 2016[37]. In the report, he offers a three-year work plan and his vision for the mandate, as well as a snapshot of the privacy landscape at the beginning of this year. As part of the Special Rapporteur's effort to facilitate further exploration and discussion of the dimensions of privacy and its relationship to other human rights, he developed an outline Ten Point Action plan.

2. In addition to Convention 108 or the CoE Convention, the Council of Europe Data Protection Convention is one of the most famous international data protection agreements in the world[38]. The Convention has been signed or is in the process of being signed by a number of countries outside of Europe, despite the fact that it was established by the Council of Europe. The Convention has been ratified by 46 Council of Europe member countries, and 46 of these countries have implemented data protection laws that comply with it (apart from Turkey, which is undergoing ratification, but the Turkish parliament recently passed a data protection law).

Non-European countries became parties to the Convention for the first time in 2013 with Uruguay. The Moroccan Government, the Senegalese Government, and the Tunisian Government are all exploring the possibility of joining the organization. Signatories are bound by the Convention, which makes it unique among global initiatives.

3. An extensive range of stakeholders was consulted by OECD member states during the development of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[39]. Their original publication was in 1980, but they were revised and reissued in 2013. Not only OECD members can follow the Guidelines, but any country can. The OECD comprises 34 member countries, 32 of which have previously adopted comprehensive data protection laws. In March 2016, the Turkish parliament passed a data protection law that should harmonize the Turkish regime with the European Union's; however, only the U.S. will be an exception (the U.S. uses sectoral approaches to data protection rather than one single law). Even though they have a real impact on privacy laws outside the OECD, the OECD Guidelines have a real impact on the content of privacy laws all over the world. Many national privacy laws are based on the eight principles contained in the Guidelines.

4. As of May 25, 2018, Regulation 2016/679 became law, also known as the General Data Protection Regulation (GDPR)[40]. It has now been explicitly adopted by every member state of the European Union. Individual rights pertaining to personal data are upheld and amended by the GDPR. These rights include the ability to access and rectify their own data, the right to erasure and deletion, the right to data portability (to be able to move it), and the right not to be impacted by automated decision making. The European Data Protection Directive addresses the transfer of personal information to third countries. Unless a third country offers adequate protection to personal data, Member States must ensure that data transfers to third countries for processing or intended processing are prohibited. Personal data may be transferred to foreign countries in accordance with Article 25(1). According to Article 26(1) and (2), data can only be processed under certain circumstances, such as if they are needed for national security. Processing by competent authorities for preventing, investigating, detaining, or prosecuting criminal offenses or enforcing criminal penalties, including preventing threats to public safety, is governed by a different legal framework.

5. Generally, EU data privacy laws presume that data processing violates data privacy, and only specific circumstances permit it to be justified. The GDPR contains extensive extraterritorial standards that apply to the processing of personal data outside the European Union regardless of the place of incorporation or principal operational region of the data controller or processor. In order to comply with the General Data Protection Regulation (GDPR), organizations outside of the European Union must handle personal information of EU residents. A controller or processor outside the European Union that processes personal data of European Union data subjects is subject to these rules under Article 3 of the GDPR[41]. Article 48 of the GDPR provides that any transfer must be made with the permission of the data subject and no disclosure can be made of data in response to a request from a foreign authority unless an international treaty has been signed with that authority allowing that disclosure. Of all the legislations worldwide, the General Data Protection Regulation of the European Union is very rigid on transfer of data to other countries.

6. For more detail, in the Asia-Pacific region there is APEC, the Asia-Pacific Economic Cooperation Framework, which is a group of 21 nations[42]. It is a cross-border privacy mechanism; privacy directives concerning personal information across borders had been in practice since the

mid-1990s when the European Union Privacy Directive was passed. The principles governing privacy as proposed by APEC are used to establish data protection, thus forming the basis of the CBPR. The CBPR System is an engaging and self-regulatory mechanism developed by APEC economies although companies in APEC member economies are not obligated to gain certification under the new Program. The CBPR system was first introduced in the United States in 2012 with the creation of the Federal Trade Commission (FTC)[43]. CBPR System reconfirms the mutual agreement on cross-border enforcement of privacy policy, the Cross-Border Privacy Enforcement Arrangement (CPEA). A third-party oversight entity, known as an Accountability Agent, has also been authorized by the Joint Oversight Panel. Member economies are not hindered by adherence by not being able to maintain their own privacy regulations; rather, Accountability Agents designate data protection authorities (DPAs) that implement the approved privacy laws. A company that is located in an economy that adheres to the CBPR framework does not need to comply with the privacy framework unless it voluntarily seeks certification. A qualified Accountability Agent must review the organization's privacy policy in order to comply with the framework. If a company's privacy policy has been approved, it meets APEC's regional privacy standards. In consequence, both the domestic authority in charge of privacy and the Accountability Agent must comply with the applicable privacy laws. By participating in the Privacy Recognition Program (PRP), processors can also obtain data controller trust by demonstrating their compliance with the CBPR System.

Measures that can be taken to prevent cross border data flows

Although connectivity and data flows offer significant economic and trade opportunities, governments are increasingly implementing data localization measures that restrict data flows[44]. Economic and trade costs will be associated with such measures. In India, Indonesia, and Vietnam, data localization measures would reduce GDP by -0.1 percent, -0.5 percent, and -1.7 percent, respectively, according to a study by Bauer et al. There are several ways in which cross-border data flow restrictions can be implemented. Data cannot be transferred outside of the country, starting from the most restrictive to the least restrictive. A copy of the data must be maintained within the country, even if the data is transferred across borders[45]. The consent of the recipient is required before global transfers can be made. Several goals drive government restrictions on cross-border data flows, including: Protecting or improving citizens' privacy ensuring rapid access to data by law enforcement. Enhancing economic growth or competitiveness Protecting or ensuring national security Leveling the regulatory playing field When designing regulations to achieve legitimate goals, government should pay particular attention to managing risk—whether to privacy, from cyberattacks, or from delays for law enforcement agencies—to a level that is acceptable relative to the economic and social benefits, including innovation, these activities are expected to bring about. In most cases, data localization is suboptimal in that legitimate regulatory goals can be achieved with less impact on economic growth and trade, depending on the government's acceptable level of risk. Overall domestic investments are negatively impacted by data localization requirements, resulting in slower economic growth and fewer exports.

It is detrimental to the competitiveness of both the country that implements the policies and other countries to restrict cross-border data flows. The barriers erected by one country affect other countries that rely on these data flows as well. Indian business and its individual persons can take proactive measures to address cross-border data transfer challenges:

1. Compliance Assessment: Determine who is transferring data, to whom data is being transferred, and to which countries and what laws will allow such transfers.
2. Data Minimization: Minimizing exposure to risks at the same time ensuring effectiveness in business operations by removing trans-border transfer of personal data.
3. Encryption and Data Security: One is to ensure data security throughout transfer and storage. developing and deploying high levels of security like encryption and access control.
4. Third-Party Due Diligence: There is therefore the need to ensure that third party service providers are compliant with other legal frameworks or protect relevant data before hiring them for data storage or processing.

Use of legal risk management software or the compliance management tool in India: For legal risk management one may use legal risk management software or compliance management tools. It is important for the businesses in India to know how they can transfer their data across the borders and also how they can ensure compliance. These technologies can be useful in enabling organizations to be in a position to predict and deter possible legal issues, protect personal information and respect permissions and regulation from lawyers. Implementing monitoring and regulating cross border data transfers.

DISCUSSION

In today's digital economy, cross-border data flows are the lifeblood of cross-border trade, digital services, cloud computing, and global interconnectedness. But the flow of data across boundaries is confronted with a string of legal and regulatory logjams around privacy, security, and data sovereignty. Countries have taken different approaches to dealing with data moving across borders. For example, the EU's General Data Protection Regulation (GDPR) imposes strict standards on data transfers outside the EU, including requirements for user consent, data subject rights, and adequacy determinations. By contrast, the US adopts an industry-specific model with relatively relaxed privacy measures.
India's Digital Personal Data Protection Act, 2023, represents a major departure by introducing principles of data localization, and restrictions over cross-border transfers except to the extent necessary, and if it can be proved that such transfers are secure. Despite the intention to strengthen national sovereignty and data security, these policies could erect obstacles in the operation of multinational corporations and hamper global data-driven innovation. Discrepancy between legal systems gives rise to regulatory fragmentation, and can cause compliance costs and legal uncertainty.
And the time is ripe for international cooperation to establish legal frameworks that are interoperable and strike the right balance between privacy and economic interests. By harmonizing on bilateral agreements, international treaties, or common standards to protect data independent of location, trust, efficiency, and equitable digital growth could be built around the world.

CONCLUSION

There are improved data flows across borders which results in trade, research and development and communication across borders. However, different jurisdictions adopt and implement different and sometimes contradictory legal provisions, which present great difficulties regarding data privacy and security. Lack of privacy and security, cyber threats and socially sensitive information leakage can occur if there will not be a united approach to the protection of personal data on the international level. Some countries have come up with laws such as localization to address these issues and while noble, pose problems with data transfer and connectivity. While emphasizing the requirements of the secure data flow and the protection of privacy, there is a need to achieve more coordinated agreements and standards. The study also highlights that these challenges must be

solved in order to protect the individual rights and freedoms and provide benefits for the society. The legal concerns and risks of cross border data transfer is also examined in this paper since the digital economy depends on it in executing its functions in India. Under these considerations, legal requirements are vital in the combat against the invasion of data privacy, increased compliance, and customer confidence. On this aspect, the people and organizations in India can effectively and competently handle the various cross border issues of the data transfer by employing the best practices in data protection and being conversant with the current set rules and regulations.

References

1. Dau-Schmidt, Kenneth G. "Employment in the new age of trade and technology: Implications for labor and employment law." Ind. LJ 76, 2001.
2. Caviglione, Luca, Steffen Wendzel, Simon Vrhovec, and Aleksandra Mileva. "Security and Privacy Issues of Home Globalization." IEEE Security & Privacy 20, no. 1, 10-11 2022.
3. Desierto, Diane A. "Coming Full Circle on Human Rights in the Global Economy: International Economic Law Tools to Realize the Right to Development." Loy. U. Chi. Int'l L. Rev. 18 2022.
4. Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies." Computer Law & Security Review 34, no. 1, 134-153. 2018.
5. Collie, Nicholas. "Cyber conflict and just war theory." PhD diss., University of Nottingham, 2023.
6. Burri, Mira. "Interfacing privacy and trade." Case W. Res. J. Int'l L. 53, 35 2021.
7. Abomhara, Mohamed, and Geir M. Køien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security and Mobility, 65-88. 2015.
8. Whitman, James Q. "The two western cultures of privacy: Dignity versus liberty." Yale LJ 113, 1151. 2003.
9. Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A Practical Guide, 1st Ed., Cham: Springer International Publishing 10, no. 3152676, 10-5555. 2017.
10. Bendiek, Annegret, and Magnus Römer. "Externalizing Europe: the global effects of European data protection." Digital Policy, Regulation and Governance 21, no. 1, 32-43 2019.
11. Bookert, Nyteisha, Weston Bondurant, and Mohd Anwar. "Data practices of internet of medical things: A look from privacy policy perspectives." Smart Health 26, 100342. 2022.
12. Harding, Elizabeth Liz, Jarno J. Vanto, Reece Clark, L. Hannah Ji, and Sara C. Ainsworth. "Understanding the scope and impact of the california consumer privacy act of 2018." Journal of Data Protection & Privacy 2, no. 3, 234-253. 2019.
13. Creemers, Rogier. "China's emerging data protection framework." Journal of Cybersecurity 8, no. 1 2022.
14. Gao, Raymond Yang. "A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows." Chinese Journal of International Law 22, no. 4, 707-787. 2023.
15. Lindsay, David. "An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law." Melbourne University Law Review 29, no. 1, 131-178. 2005.
16. Benson, Vladlena, Steven Furnell, Donato Masi, and Tim Muller. "Regulation, Policy and Cybersecurity." 2021.
17. Lin, Ying-Jun. "No Pay, No Gain? APEC and Taiwan's Experiences." 2023.
18. Cunha, Rossana, Thiago Castro Ferreira, Adriana Pagano, and Fabio Alves. "A Persona-Based Corpus in the Diabetes Self-Care Domain-Applying a Human-Centered Approach to a Low-

Resource Context." In Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024), pp. 1353-1369. 2024.
19. Casalini, Francesca, and Javier López González. "Trade and cross-border data flows." 2019.
20. Pepper, Robert, John Garrity, and Connie LaSalle. "Cross-border data flows, digital innovation, and economic growth." The Global Information Technology Report 2, 39-47, 2016.
21. Singh, Seema. "Regulation Of Cross-Border Data Flow And Its Privacy In The Digital Era." NUJS Journal of Regulatory Studies 9, no. 2 2024.
22. Simangunsong, Eliot, and Rudy Handoko. "The Role of Social Media in Business Transformation Strategies (Development and Validation of the Social Media Commerce Model)." In 3rd Asia Pacific Management Research Conference (APMRC 2019), pp. 224-231. Atlantis Press, 2020.
23. Rengel, Alexandra. "Privacy as an international human right and the right to obscurity in cyberspace." Groningen Journal of International Law 2, no. 2 2014.
24. Voss, W. Gregory. "Cross-border data flows, the GDPR, and data governance." Wash. Int'l LJ 29, 485. 2019.
25. Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A Practical Guide, 1st Ed., Cham: Springer International Publishing 10, no. 3152676, 10-5555. 2017.
26. Meltzer, Joshua Paul. "The I internet, Cross-Border Data Flows and International Trade." Asia & the Pacific Policy Studies 2, no. 1, 90-102, 2015.
27. Wong, Richmond Y., Andrew Chong, and R. Cooper Aspegren. "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures." Proceedings of the ACM on Human-Computer Interaction 7, no. CSCW1, 1-26 2023).
28. Basu, Subhajit, and Richard Jones. "E-commerce and the law: a review of India's Information Technology Act, 2000." Contemporary South Asia 12, no. 1, 7-24, 2003.
29. Asawat, Vikas. "Information technology (Amendment) act, 2008: A new vision through a new change." Available at SSRN 1680152 2010.
30. Asawat, Vikas. "Information technology (Amendment) act, 2008: A new vision through a new change." Available at SSRN 1680152 2010.
31. Sullivan, Clare. "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era." computer law & security review 35, no. 4, 380-397. 2019.
32. Watt, Eliza. "The right to privacy and the future of mass surveillance." The International Journal of Human Rights 21, no. 7, 773-799. 2017.
33. Bogecho, Dina. "Putting it to good use: the international covenant on civil and political rights and women's right to reproductive health." S. Cal. Rev. L. & Women's Stud. 13, 229. 2003.
34. Damen, Juliane, Lena Köhler, and Sean Woodard. The human right of privacy in the digital age. No. 3. Universitätsverlag Potsdam, 2017.
35. Hansen, Marit. "Interview with the UN special rapporteur on the right to privacy: Mission impossible? No. Joe Cannataci is quietly confident and comes well-equipped." Datenschutz und Datensicherheit-DuD 39, no. 12, 786-788, 2015.
36. Hannum, Hurst. "The status of the Universal Declaration of Human Rights in national and international law." Ga. J. Int'l & Comp. L. 25, 287, 1995.
37. Rotenberg, Marc. "Urgent mandate, unhurried response: an evaluation of the UN Special Rapporteur on the right to privacy." Eur. Data Prot. L. Rev. 3, 37 2017.

38. Greenleaf, Graham. "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108." International Data Privacy Law 2, no. 2, 68-92, 2012.
39. Kirsch, William J. "The protection of privacy and transborder flows of personal data: the work of the Council of Europe, the Organization for Economic Co-operation and Development and the European Economic Community." Legal Issues of Economic Integration 9, no. 2 1982.
40. Regulation, General Data Protection. "GDPR. 2019." 2019.
41. De Hert, Paul, and Michal Czerniawski. "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." International Data Privacy Law 6, no. 3, 230-243. 2016.
42. Rudner, Martin. "APEC: the challenges of Asia Pacific economic cooperation." Modern Asian Studies 29, no. 2, 403-437. 1995.
43. Sullivan, Clare. "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era." computer law & security review 35, no. 4, 380-397. 2019.
44. Tuthill, L. Lee. "Cross-border data flows: What role for trade rules?." In Research handbook on trade in services, pp. 357-382. Edward Elgar Publishing, 2016.
45. Svantesson, Dan Jerker B. "The regulation of cross-border data flows." Int'l Data Priv. L. 1, 180, 2011.