

Transborder Data Transfers: Effects on Developing Nations and Security Implications for Personally Identifiable Information (PII)

CHIEMEZIE MAXIMILLIAN UZOHO¹, PAUL AYAMBE NDIK², ZULAIHAT MUKHTAR³,
USMAN SHETTIMA SHETTIMA⁴, HABIBA BAGUDU⁵
^{1, 2, 3, 4, 5} National Space Research and Development Agency (NASRDA)

Abstract- *Transborder data transfers have become fundamental to the global digital economy, facilitating international trade, cloud computing, and the delivery of digital services. This paper analyzes the implications of such transfers for developing nations, with particular emphasis on the security of Personally Identifiable Information (PII). While cross-border data flows enable firms in developing economies to access international markets, cloud infrastructure, and digital platforms, they simultaneously expose these states to regulatory and cybersecurity vulnerabilities. Empirical evidence indicates a significant governance gap: only 73% of developing countries have enacted data-protection legislation compared to 98% of developed countries. This disparity, coupled with limited technical and institutional capacity, heightens the risk of unauthorized access, data breaches, and misuse of PII.*

Furthermore, the fragmentation of international data-protection regimes creates legal uncertainty, as PII may be processed under jurisdictions with divergent privacy standards. The study argues that the effects of transborder data transfers are contingent upon the strength of legal, institutional, and technological safeguards. For developing nations to derive developmental benefits while mitigating risks, it is imperative to establish trusted data-governance frameworks that ensure accountability, interoperability, and adequate protection of PII within the global digital ecosystem.

Keywords: *transborder data transfers, developing nations, pii, data protection, cybersecurity, governance*

I. INTRODUCTION

The rapid expansion of digital technologies has transformed data into a critical resource for economic activity, public administration, scientific research and international commerce. The increasing use of cloud computing, digital platforms, online financial services,

telecommunications and globally distributed information systems has consequently made the movement of data across national boundaries an integral component of the contemporary digital economy. Transborder data flow support international business operations, supply chains, communication and digital trade, while also creating complex questions concerning privacy, cybersecurity, regulatory jurisdiction and national security .

The significance of transborder data transfers extends beyond the movement of information between geographically separated computer systems. Data increasingly functions as an economic and strategic asset capable of generating both private and social value. and argues that the growing importance of data has implications not only for international trade and economic development but also for human rights, peace, security and the distribution of economic benefits. Consequently, the governance of cross border data flows has become an important policy issue, particularly for developing nations seeking to participate more extensively in the global digital economy .

A particularly sensitive dimension of transborder data transfer concerns personally identifiable information (PII). PII encompasses information that can identify an individual directly or that can reasonably be associated with an identifiable person. Examples may include names, identification numbers, financial information, contact details, biometric information, location information and other personal attributes. When such information crosses national borders, its protection becomes more complicated because the data may subsequently be stored, processed or accessed under a legal and regulatory framework different from that of the country where it was originally collected. identifies the interoperability of privacy and data-

protection frameworks as one of the central challenges associated with trusted cross-border data flows.

For developing nations, transborder data transfers present both developmental opportunities and significant risks. International data flows can enable firms in developing economies to participate in global digital services, access foreign markets, use international cloud and computing infrastructure, and receive digitally delivered services. At the same time, restrictions on such flows can impose economic costs on businesses and limit their ability to participate in international digital markets.

The developmental benefits, however, must be considered alongside differences in technological, regulatory and institutional capacity. Developing countries may face difficulties establishing and enforcing comprehensive data-protection regimes, particularly where there are limitations in technical expertise, institutional resources and cybersecurity capacity. Current data from the UNCTAD Global Cyberlaw Tracker illustrates this disparity: as of its current assessment, data-protection and privacy legislation is recorded for 73% of developing countries compared with 98% of developed countries .

The regulatory environment governing transborder personal-data transfers is also highly fragmented. Countries have adopted different approaches to determining when personal information may leave their jurisdictions. Broadly, these approaches include open transfers, conditional transfers and limited transfers . Conditional regimes, for example, may permit international transfers only when particular safeguards, contractual arrangements, adequacy requirements or other protective measures are satisfied. Such differences can create compliance difficulties for organizations operating across multiple jurisdictions while simultaneously creating uncertainty about the level of protection afforded to individuals once their information leaves the country of origin.

The security implications are particularly important because the transfer of PII creates additional points at which information may be exposed to unauthorized access, interception, misuse or compromise. Cross-border processing may involve multiple organizations, cloud providers, data centres and jurisdictions,

potentially increasing the complexity of determining responsibility when a security incident occurs. The OECD therefore emphasizes the need to facilitate international data flows while ensuring that data continues to receive appropriate oversight and protection after crossing national borders .

The paper argues that transborder data transfers are neither inherently beneficial nor inherently harmful; their consequences depend substantially on the legal, institutional and technological safeguards governing the collection, transfer, processing, storage and protection of personal information. For developing nations, the objective should therefore be to establish a trusted data-governance environment capable of protecting PII while enabling participation in the global digital economy.

II. TRANSBORDER DATA TRANSFERS CONCEPT AND GLOBAL LANDSCAPE

Transborder data transfer refers to the movement of data from one national jurisdiction to another for purposes such as storage, processing, analysis, communication or service delivery. The concept is closely associated with the broader phenomenon of cross-border data flows, through which information moves between organizations, individuals, digital platforms and infrastructure located in different countries. Such flows have become fundamental to international business, logistics, global supply chains, communication and digital trade .

The increasing internationalization of data is partly a consequence of the distributed architecture of contemporary digital services. A single digital transaction may involve the collection of PII in one country, processing by a service provider in another, storage in a third country and subsequent access by an organization located elsewhere. Cloud computing and globally distributed data infrastructures have further increased this geographic dispersion. Consequently, the physical location of data is increasingly separated from the location of the individual or organization from which the data originated ; .

Nature and Importance of Transborder Data Transfers

Cross-border data movement serves several important economic and technological functions. Multinational

organizations use international data transfers to coordinate operations, manage customers, process payments, conduct research, provide cloud-based services and maintain global supply chains. Developing countries can also use these flows to access international digital infrastructure and participate in global digital markets. consequently, considers cross-border data flows an important component of the contemporary digital economy, while emphasizing that their benefits and risks are distributed unevenly among countries.

The significance of these transfers becomes particularly apparent when considering the increasing reliance on cloud computing and data-intensive digital services. An organization may not know, or may not directly control, the physical jurisdiction in which particular categories of data are processed at a given moment. This creates additional governance challenges because the legal protection applicable to the information may change when it crosses a national boundary.

For PII, this distinction is particularly important. The transfer of personal information outside the jurisdiction where it was initially collected may expose the information to different privacy requirements, government-access rules, security standards and enforcement mechanisms. The consequently identifies interoperability among privacy and data-protection frameworks as a major component of establishing trustworthy international data flows.

Global Regulatory Approaches

There is currently no single global regulatory framework governing transborder transfers of personal data. Instead, countries have developed different approaches based on their economic priorities, privacy traditions, national-security concerns and institutional capacities. ; describe the resulting international environment as a patchwork of rules and mechanisms that can complicate compliance and increase the costs associated with operating across jurisdictions.

Transborder data transfers are broadly categorized by national approaches to international transfers of personal data into three distinct models open transfers, conditional transfers and limited transfers. These

models represent different balances between facilitating international data movement and maintaining regulatory control over personal information.

Data Localization and Data Sovereignty

The emergence of data-localization requirements reflects growing concerns about privacy, cybersecurity, government access to information and national sovereignty. Governments may seek to retain greater control over data generated within their territories by requiring organizations to maintain domestic copies or restricting the transfer of certain categories of information abroad.

However, localization does not automatically guarantee stronger data security. notes that localization requirements can create additional costs and may have implications for the efficiency and resilience of data-management systems. Therefore, the physical location of data should not be regarded as a substitute for effective cybersecurity, privacy governance and institutional oversight.

For developing nations, this distinction is particularly important. Mandatory localization may strengthen governmental control over sensitive information, but it can also require substantial investment in domestic data centres, cybersecurity infrastructure and technical expertise. A country may consequently achieve greater territorial control over data without necessarily possessing the institutional capacity required to protect it effectively .

III. EFFECTS OF TRANSBORDER DATA TRANSFERS ON DEVELOPING NATIONS

Transborder data transfers have become increasingly important to the economic and technological development of developing nations. The ability to move data across jurisdictions enables organizations to access international markets, cloud-computing infrastructure, digital platforms, financial services and global supply chains. However, the effects are not uniformly positive. While international data flows can facilitate economic growth and technological development, they can also deepen technological dependency, expose domestic populations to privacy and cybersecurity risks, and create regulatory

challenges for countries with limited institutional capacity ; .

Economic and Digital Development Opportunities

One of the principal benefits of transborder data transfers is their contribution to digital trade and international economic participation. Businesses increasingly require the ability to transfer data across borders to communicate with customers, process transactions, coordinate employees and manage international supply chains. Restrictions that unnecessarily prevent such transfers can therefore increase operational costs and limit the ability of domestic firms to participate in global markets .

For developing nations, this capability can be particularly valuable because digital services provide opportunities to participate in global markets without requiring the same level of physical infrastructure traditionally associated with international trade. Cross-border data flows can support sectors such as financial technology, business-process outsourcing, telecommunications, e-commerce, software development and digital professional services. emphasizes that effective data governance can allow countries to derive economic and social value from data while supporting participation in the global digital economy.

The relationship between data flows and development is therefore potentially significant. International data movement allows businesses located in developing countries to interact with customers and service providers abroad, while access to international digital infrastructure can reduce the need for every country to independently develop all of the computing and storage resources required by modern digital services.

Data Sovereignty and Digital Dependency

A further concern is data sovereignty. As more personal and commercially valuable information is transferred to foreign jurisdictions, developing countries may become increasingly dependent on external infrastructure and foreign technology providers. This dependency can extend beyond data storage to include cloud platforms, software, cybersecurity services, data analytics and artificial-intelligence infrastructure.

Such dependence does not necessarily represent a security problem by itself. However, excessive dependence can reduce a country's ability to exercise independent control over critical information infrastructure. argues that the global data economy is characterized by significant concentration of data, digital platforms and technological capabilities, raising concerns about unequal distribution of economic value and technological power.

For developing nations, the issue is consequently not simply where data is stored, but also who controls the infrastructure, technologies and processes through which the data is collected, transferred and monetized.

Privacy and Cybersecurity Risks

The international movement of data also increases the complexity of protecting PII. Once information crosses a national boundary, it may be processed by additional organizations and become subject to different legal requirements. This can make it more difficult for individuals to understand how their information is being used and where it is stored.

The security challenge is further complicated by the possibility of cyberattacks targeting organizations involved in international data processing. A breach at a cloud provider, data processor, telecommunications provider or other intermediary can potentially expose information belonging to individuals from several countries simultaneously . For developing nations, the consequences may be particularly severe where cybersecurity capabilities are limited. A country may have legislation governing personal information but lack sufficient technical resources to detect sophisticated attacks, investigate breaches or enforce security requirements effectively .

IV. SECURITY IMPLICATIONS OF TRANSBORDER DATA TRANSFERS FOR PERSONALLY IDENTIFIABLE INFORMATION

The international movement of personally identifiable information (PII) creates security challenges that extend beyond the conventional protection of data within a single jurisdiction. When PII moves across national borders, it may pass through multiple networks, service providers, cloud platforms and legal

environments. Each additional point of processing or storage can introduce new opportunities for unauthorized access, misuse, interception or compromise. Consequently, the security of transborder PII depends not only on the security controls implemented by the organization collecting the information but also on the practices of every entity involved in its subsequent transfer and processing .

The issue is particularly important because PII has significant value to cybercriminals and other malicious actors. Compromised personal information can be used for identity theft, financial fraud, social engineering, targeted attacks and unauthorized profiling. The cross-border nature of modern digital services can make these risks more difficult to detect, investigate and remedy because the affected individuals, data controllers, processors and infrastructure may be located in different jurisdictions .

Unauthorized Access and Data Breaches

One of the most significant security risks associated with transborder PII is unauthorized access. Personal information transferred to foreign organizations or third-party processors may be exposed if appropriate authentication, access-control and cybersecurity measures are not maintained throughout the data lifecycle.

The problem is particularly pronounced in cloud-based environments. A single service provider may process information belonging to individuals from numerous countries, meaning that a successful compromise can expose large volumes of internationally sourced personal information simultaneously. therefore, emphasizes the importance of ensuring that privacy and security protections remain effective when data is transferred between jurisdictions.

A data breach involving transborder PII can also create complex questions concerning responsibility. Determining which organization is responsible for securing the information, notifying affected individuals and cooperating with authorities may become difficult when several organizations operate under different national laws. Regulatory

fragmentation can therefore transform a technical security incident into a broader legal and governance problem .

Loss of Control Over Personal Information

A fundamental consequence of transborder data transfer is the potential reduction in an individual's practical control over their information. Once PII has been transferred to another jurisdiction, the individual may have limited ability to determine where it is stored, who processes it, how long it is retained or whether it is transferred again to another organization.

This is particularly challenging when different jurisdictions provide different levels of privacy protection. An individual may provide information to an organization under the assumption that it will receive a particular level of protection, only for that information to subsequently be processed in an environment governed by substantially different requirements.

It is important that in the transfer of personal data across geographically distinct nations, maintaining trust in cross-border data flows through compatible privacy frameworks and appropriate safeguards must be ensured. The objective is to prevent international transfer from becoming a mechanism through which organizations can circumvent stronger privacy requirements simply by moving information to another jurisdiction .

Third-Party and Supply-Chain Risks

Transborder PII frequently involves third parties. An organization may collect information directly from individuals but rely on external cloud providers, analytics companies, payment processors, customer-management platforms or other service providers to process it.

Each additional organization introduces another potential point of compromise. Moreover, the original data controller may have limited visibility into the security practices of every organization involved in the data-processing chain. This creates a data supply-chain risk, in which the security of an organization's PII depends partly on the security practices of external entities.

The OECD (2022) emphasizes the importance of accountability and appropriate safeguards throughout cross-border data-processing arrangements. Consequently, organizations transferring PII internationally should conduct appropriate assessments of third-party security practices and establish contractual and technical controls governing how transferred information may be processed.

Security Implications for Developing Nations

The risks described above may be amplified in developing nations where cybersecurity and data-protection institutions have comparatively limited resources. UNCTAD's Global Cyberlaw Tracker demonstrates continuing differences in the adoption of data-protection and privacy legislation between developed and developing countries

However, the issue should not be interpreted simply as a question of whether developing countries should prevent their citizens' information from leaving national territory. Data localization can provide greater territorial control but does not automatically eliminate cyber threats, insider risks or poor security practices. Instead, effective protection requires a combination of technical safeguards, legal requirements, institutional oversight and organizational accountability.

This distinction is critical. The security of PII ultimately depends more on the quality of controls surrounding the information than merely on the geographical location of the server on which it resides.

V. REGULATORY AND GOVERNANCE CHALLENGES

The protection of personally identifiable information (PII) during transborder data transfers depends heavily on the regulatory and governance mechanisms established by countries and organizations. While technical controls such as encryption, authentication and access management are essential, they cannot independently resolve questions concerning jurisdiction, accountability, lawful data processing, government access and individual rights. The international nature of data flows therefore creates a governance challenge in which multiple legal systems

may apply to the same information at different stages of its lifecycle .

For developing nations, this challenge is particularly significant because regulatory frameworks and institutional capacities may not have developed at the same pace as digital technologies. The result can be a mismatch between the growing volume of personal information crossing national borders and the ability of governments to effectively regulate and protect that information.

Fragmentation of Data-Protection Laws

One of the principal governance challenges is the fragmentation of national data-protection regimes. Countries differ in their definitions of personal data, requirements for lawful processing, individual rights, breach-notification obligations, regulatory powers and conditions for international transfers. Although there are important areas of convergence among national frameworks, significant differences remain .

This fragmentation creates uncertainty for organizations that transfer PII across multiple jurisdictions. A transfer that satisfies the requirements of one country may require additional safeguards under the laws of another. Consequently, multinational organizations may have to establish complex compliance programmes to determine which rules apply to specific categories of information and particular transfer arrangements.

For developing countries, regulatory fragmentation can also make it difficult to negotiate compatible arrangements with larger economies. Countries with limited legislative and technical expertise may have difficulty demonstrating that their domestic data-protection frameworks provide safeguards comparable to those required by foreign jurisdictions.

VI. CONCLUSION

Developing Nations are beginning to gain insight into the importance and relevance of data. The harvesting, processing, storage and control is beginning to get attention to developing Nations especially in Africa. But these nations face challenges regarding capacity and technology to effectively collect, process and store the ton of data its citizenry possess. Developed nations

have through its institutions (private and public) gained relevant insights into the developing nations as a result of the data they collect. Most developing Nations host their servers and other critical national assets such as ground satellite stations abroad where they believe it is most secured and less susceptible to manipulations. This reasoning has further advanced the position of the host nations in regards to how they can take advantage of the information they have harvested from these data.

Transborder data transfer therefore poses most of the risks to the disadvantaged developing nations who will have to rely on the technical expertise of far more advanced nations in deploying technologies capable of collecting personal identifiable information of developing nations. Therefore, it is pertinent that international laws and guidelines must be in place to protect data of developing nations stored far from their physical geographical reach.

REFERENCES

- [1] Belli, L., Gaspar, W. B., & Jaswant, S. S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*.
- [2] Casalini, F., & González, J. L. (2019). OECD Trade Policy Papers. *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers.
- [3] Fratini, S., & Musiani, F. (2024). Data localization as contested and narrated security in the age of digital sovereignty: the case of Switzerland. *Information, Communication & Society*, 1368-1386.
- [4] Hand, D. J. (2018). Aspects of Data Ethics in a Changing World: Where Are We Now? *Big Data*.
- [5] Kuner, C. (2010). Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future. *TILT Law & Technology Working Paper*.
- [6] Laidlaw, E. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. *Available at SSRN 3790936*.
- [7] Mitchell, A. D., & Mishra, N. (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. *Journal of International Economic Law*, 389–416.
- [8] Osakwe, P. N., & Solleder, O. (2023). Wealth Distribution, Income Inequality and Financial Inclusion: A Panel Data Analysis. *UNCTAD Working Paper*.
- [9] Peltola, A., Barnat, N., & MacFeely, S. (2022). The role of international organizations in statistical standards setting and outreach: An overview of the UNCTAD contribution. *Statistical Journal of the LAOS*.
- [10] Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. *Journal of International Business Policy*, 10–32.
- [11] Sauvart, K. P. (2009). Transborder data flows and the developing countries. *International Organization*, 359 - 371.
- [12] Shi, Y. (2025). Risk Prevention in Global Cross-Border Data Flows: Challenges and China's Strategic Responses. *International Journal of Digital Law and Governance*.
- [13] Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*.
- [14] Tran, E., & Atkinson, M. (2002). Security of personal data across national borders. *Information and Computer Security*, 237-241.
- [15] Wilson, J. M. (2022). Cross-Border Data transfers: A Balancing Act through Federal Law. *Entrepreneurship & Tax L. Rev.*
- [16] Wilson, L. J., & Al-Muhanna, I. (1985). The Political Economy of Information: The Impact of Transborder Data Flows. *Journal of Peace Research*.
- [17] Zhang, C., Liu, Y., Xu, M., Yang, X., Li, P., & Yang, C. (2025). Trans-Border Trusted Data Spaces: A General Framework Supporting Trustworthy International Data Circulation. *IEEE Access*, 30481 - 30496.