International Journal of Law and Society
2026, Vol. 9, No. 3, pp. 346–352
https://doi.org/10.11648/j.ijls.20260903.14

SciencePG
Science Publishing Group

Research Article

Navigating the Complexities of Cross-Border Data Transfers: Impacts on Multinational Enterprises and Strategic Responses to Regulatory Discrepancies

Amos William Omolo*

Managing Partner, William & Case Associates, Nairobi, Kenya

Abstract

Modern social and economic relations depend on data as the basis of global trade, digital services, and the operations of MNEs. However, the rapid expansion of cross-border data flows has intensified concerns regarding privacy, security, and regulatory oversight, particularly as data increasingly diffuses across multiple jurisdictions. Countries have in turn pursued divergent regulatory solutions, such as data localization policies and transfer limits, leading to a great deal of fragmentation in data governance globally. The paper will discuss differences in regulatory practices in major jurisdictions and discuss the implications of such differences on the operations of MNEs. Based on the institutional logics theory, it describes how divergent policy frameworks are created by existing national priorities, including privacy security, economic liberalization, and national security. The research uses a qualitative document review of policy documents, regulatory tools, and a subset of case-based evidence to determine essential trends and effects. The findings show that, fragmentation of regulations increases compliance costs, operational inefficiencies, and uncertainty of the law to MNEs. In reaction, some adaptive strategies are taken by the firms, such as localized data management and compliance systems, and policymakers are willing to have more international coordination. The paper adds to the body of writing on international business and data governance on the importance of additional interoperable regulatory frameworks that would facilitate the balance between data mobility and trust and protection.

Keywords

Cross-border Data Flows, MNEs, Data Governance, Regulation

1. Introduction

International transfers of information are the backbone of the global economy since they allow businesses and consumers to obtain high-quality services and technologies no matter where they are. There are cross-border data flows that generate value in various industries such as financial services, healthcare, manufacturing, and education [1]. For firms operating in international markets, continuous and reliable access to data is essential for managing global workforces, coordinating supply chains, and delivering goods and services efficiently. The growth in digital technologies has also allowed micro-MNEs to access the global market and compete on a non-geographical level [1]. But as companies go global, the necessity to move data across borders creates serious questions concerning data security, privacy, and data adherence to

*Correspondence: Amos William Omolo (william@williamcase.co.ke)

Received: 26 November 2025; **Accepted:** 6 May 2026; **Published:** 6 August 2026

different regulatory standards. As governments continue to put more focus on personal data protection, the regulation of cross-border data flow has become a central issue of concern to firms operating internationally [2].

2. Significance and Contribution of the Study

This study contributes to the literature on international business and data governance by examining how regulatory discrepancies in cross-border data flows affect MNEs and by identifying strategic responses to these challenges. Since MNEs are increasingly relying on data as a decision-making mechanism and to be efficient in their operations, it is vital to comprehend the consequences of fragmented regulatory environments to remain competitive. The paper describes in more detail the practical implication of convergent regulatory frameworks in terms of implications for the cost of compliance, the efficiency, and the strategies. Also, it presents the interplay between the firm strategies and the public policies response by reflecting and provides a framework that provides an integration of institutional logics, and international business strategies. In consequence, the study is not only contributing to the academic knowledge about the operations of the MNEs in the environment of regulatory complexities but also offers policymakers alternatives that may - at least - help to make the global data flow more efficient and safer.

3. Research Gap

While there is much literature on the subject of cross-border data regulation, little attention has been given to the effects of differences in regulation on the operational and strategic functions of the MNEs. Much of the previous research is on regulatory structure, or impacts on the economy of data localization, which does not take into account the operational issues and the reaction policy of the firms [10]. This gap is bridged in this research paper as it provides a parsimonious analysis of the effects of various regulatory systems on the behavior of MNEs and examines the various strategic reactions that firms and policymakers have taken to manage these complexities.

4. Theoretical Framework

The study is grounded on the institutional theory, that is, on the notion of institutional logics, which explains how different institutional settings impact organizational behavior and strategic decision making. Though the traditional institutional theory puts an emphasis on convergence in organizational practices, there are also institutional logics that emphasize the coexistence of multiple and in certain situations, conflicting rationality both within and across societies [3]. The different fields within the society, such as markets, states, and communities give birth to these logics, and they can undergo heterogeneous practices of regulation and organization responses.

The institutional logics would be an excellent approach when it comes to the selection of country to pursue in the context of cross-border data governance. As an illustration, oversight of data protection and privacy is valued more in certain jurisdictions; meanwhile, market efficiency or national security is at a higher priority in others. These contradictory priorities can affect the choice of policies and result in the issue of fragmented regulations in various areas. This leads to the operations of MNEs in many countries to face a range of regulatory challenges [10]. This article uses the institutional logics theory to navigate such diversity in regulation, its impact on policymakers and firms. This paper examines how governments respond to multiple and competing pressures creating data governance regimes and how MNEs elaborate on their strategies in these new institutional settings. The framework offers a suitable perspective to study the interplay of regulatory diversity and firm-level strategic adaptations through the concept of institutional logics for cross-border data regulation.

5. Methodology

The research used qualitative document analysis methodology to reveal the regulatory concerns of cross-border data flows and implications to the MNEs. The approach is the systematic review of the secondary sources to identify patterns, themes and strategies in wide range of regulatory settings.

5.1. Literature Review and Data Sources

The theoretical and empirical framework of this research was set out through a review of the literature, policy papers and reports. Academic journals, journals of international institutions and policy briefs on global data governance, MNEs and digital trade were considered. Academic publications through Google and institutional databases were used as the main sources; and, as a complement to these sources, documents from agencies such as OECD and other policy agencies were used.

5.2. Document Selection Criteria

The selection of documents is based on relevance, quality and time period. The part of the literature that had content related to international data transfers, regulatory frameworks and how they affect MNEs were inclusion criteria, particularly in Africa, the EU, the US and China. Only well-articulated, rigorous and elaborated sources were funneled. It also looked at all the documents published since 2014 for the review to pinpoint the recent trends in regulatory practices.

5.3. Data Analysis Procedure

The documents received were content analyzed through a

thematic analysis. This entailed categorizing the information to bring out the main themes which include the differences in regulatory environments, institutional logics, firm compliance and actions taken by MNEs. Themes were refined and this helped to increase their consistency and marital to the purposes of the research.

5.4. Synthesis and Interpretation

The results of the thematic analyses were condensed and described in an attempt to capture the total picture of the effect of regulatory fragmentation on operations and decision-making in MNEs. The problem of the different companies' adaptations to the varying regulatory regimes and the role of the policy setting in the adaptation were also investigated.

5.5. Formulation of Recommendations

To make practical recommendations to MNEs and policymakers, based on the findings, the synthesized findings were formulated. The recommendations were grounded on the outlined tendencies in the literature stream and aimed to maximize regulatory harmonization, grow compliance, and simplify the process of cross-border data flows.

6. Complexities of Cross-Border Data Transfers

6.1. Regulatory Discrepancies Among African Countries

The high level of regulatory fragmentation is also intrinsic to Africa, especially in the area of cross-border data management, which leads to the lack of unity in the legislation, the enforcement mechanisms, or the compliance criteria. These differences reflect the institutional priorities and differences in regulatory capacity and result in a complicated environment of MNEs operating on the continent [4]. For example, while Ghana and Mauritius impose penalties for non-compliance with data protection requirements, other countries such as Senegal, Nigeria, Tunisia, and Morocco do not consistently require notification of violations [4]. Likewise, in Kenya, the DPA mandates that the data controller must establish sufficient protection measures prior to relocating personal information to a foreign country, usually on the basis of consent, sufficiency ruling, or necessity [5].

Table 1. *Comparative Overview of Data Protection Frameworks in Selected African Countries.*

Country	Key Legislation	Data Localization	Consent Requirement	Transfer Mechanism	Key Challenges
Kenya	Data Protection Act (2019)	Partial	Explicit consent	Safeguards, adequacy, agreements	Strict compliance requirements
Nigeria	Data Protection Act (2023)	Yes	Required	Conditional transfer approvals	High compliance costs
Zambia	Data Protection Act (2021)	Yes	Required	Ministerial approval	Regulatory uncertainty
Botswana	Data Protection Act (2018)	Limited	Conditional	Approved country list	Lack of transparency
South Africa	POPIA (2013)	No	Required	Consent, contracts, benefit test	Complex compliance structure
Eswatini	Data Protection Act (2022)	Partial	Required	SADC-based framework	Regional inconsistency
Somalia	Data Protection Act	No	Required	Consent-based	Weak regulatory clarity

Stricter approaches are implemented in Nigeria and Zambia, where data localization is required, meaning that some of the types of personal data have to be stored within the country [11]. Botswana permits government discretionary approval of transfer destinations, whereas the POPIA in South Africa permits transfers on conditions like consent, contractual protections, and proving that they are of benefit to the data subject [5]. Eswatini also makes the data flows more complicated by distinguishing the SADC countries and non-SADC ones, which contributes to extra conditions in external transfers. Somali, on the other hand, focuses more on informed consent and has no explicit statements on how to localize data [6]. Such differences produce a disjointed regulatory environment, which compounds the complexity of compliance, interoperability, and increases the cost of operation among MNEs.

6.2. Regulatory Discrepancies: The EU, the US, and China

Differences in regulatory regimes between distinct economies at the international stage are even more salient where institutional logics are quite dissimilar [12]. The EU is a right-

based concept and privacy is deemed as a right of human being. The implementation of the GDPR has necessitated tough requirements on the cross-border transfer of data provisions, and the provisions of adequacy are required and there are protection options including standard contractual terms and protection by binding corporate rules [3]. Despite being a good source of data protection, such measures impose more compliance burdens on firms.

The U.S follows a market-based framework, which is marked by a diffused system of sector-specific rules [13]. It promotes relatively free data flows to develop its digital economy and privacy protections are balanced against economic objectives. International data regulation is complicated by the fact that the legislative tools like the CLOUD Act that widen the extraterritorial reach of the U.S. jurisdiction have been used [3]. China is more state-oriented with national security and data sovereignty being its priorities [13]. The regulatory framework, to which it is applied, is the CSL, DSL, and PIPL, which introduce strict data localization requirements and huge government control over the cross-border data transfer [3].

Table 2. *Comparative Analysis of Data Governance Models.*

Region	Core Logic	Key Laws	Data Flow Approach	Key Features	Impact on MNEs
EU	Privacy as a right	GDPR	Restrictive	Strict safeguards, adequacy requirements	High compliance costs
US	Market-driven	CCPA/CPRA, CLOUD Act	Liberal	Sectoral laws, flexible transfers	Operational flexibility
China	National security	CSL, DSL, PIPL	Highly restrictive	Data localization, state oversight	Infrastructure restructuring

6.3. Implications for MNEs

The work of MNEs in the sphere of regulatory practices is greatly influenced by jurisdictional fragmentation in the area. To start with, the companies will need to incur higher costs on compliance since they are expected to implement different systems of regulation and invest into legal capabilities, infrastructure and data protection systems [3]. Second, low operational efficiency exists as firms have to cope with complex and even chaotic demands that exist across jurisdictions. Third, legal uncertainty amplifies business risk because of the fluctuating and conflicting regulations.

Moreover, regulatory differences may limit innovation and affect strategic choices such as market entry and where to invest. Companies usually prefer jurisdictions that have foreseeable regulatory landscapes and lax data policies [7]. An example is how strict GDPR requirements have made it more expensive to comply with the regulations, especially by companies like Meta, and U.S. China regulatory conflicts have compelled companies like Apple to reorganize data storage and processing systems [3].

6.4. Planned Reactions to Regulatory Tidiness

6.4.1. MNE Strategies

In order to deal with these issues, MNEs implement a number of strategies:

1) Formulation of elaborate compliance mechanisms to check regulatory changes.
2) Hypothesis: Investing in localized and distributed data infrastructure.
3) Adoption of enhanced encryption and data protection systems.
4) Assessment of market entry on the basis of regulatory risk.

6.4.2. Policy and Institutional Responses

Multilateral cooperation at the policy level is needed to minimize regulatory fragmentation. Policies like the World Trade Organization are essential for promoting the infrastructure for international balancing of data protection, economic growth, and national interests [7].

Table 3. *Strategic Responses by MNEs and Policymakers.*

Actor	Strategy	Example	Benefits	Challenges
MNEs	Compliance systems	Internal data governance teams	Reduced legal risk	High cost
MNEs	Data localization	Local data centers	Regulatory compliance	Infrastructure cost

Actor	Strategy	Example	Benefits	Challenges
MNEs	Encryption & security	Advanced cybersecurity systems	Data protection	Technical complexity
Governments	Regulatory harmonization	Trade agreements	Easier data flows	Political differences
Institutions	Global frameworks	WTO initiatives	Standardization	Limited enforcement

7. Discussion

By November 2023, 35 African countries had adopted data protection laws, with three countries having data protection bills awaiting approval [5]. Majority of these frames allow cross-border data transfers under the conditions of consent and presence of sufficient data protection in recipient countries. This, though a pointer of a general need to promote data flows, interpretative variation, implementation and institutional capacity is a big challenge to MNEs [14]. This kind of contradictions conforms to the theory of institutional logs, and some countries give more emphasis to either privacy, economic development or regulation control that results in unequal governance effects.

The regional level of cross-border data governance is not highly developed [17]. The AfCFTA lacks binding data flows across borders but it is addressed within the Digital Trade Protocol [8]. Similarly, regional groupings such as TFTA do not have many alternatives with regard to coordination. The most widespread tool that would be implemented by the continent is the Malabo Convention which, however, is biased and addressed primarily to the member states [15]. This leads to regulatory fragmentation in the continent as a consequence of the availability of different regional arrangements and country specific structures.

Examples of how various institutional logics affect the regulatory reaction to cross-border data flows across the globe include the EU, the US and China [3]. EU represents privacy as the primary right, the US is interested in market efficiency and innovativeness, and China in national security and sovereignty over data. The existing differences can be attributed not only to the fact that the ideological and economic priorities are different but also to the fact that the realization of regulatory convergence remains a challenge [7]. These conflicting approaches are only going to intensify, with more and more development of digital technologies, and with the growing problem of global data regulation becoming more complicated [16].

Countries should seek aligned policy solutions that consider privacy, security, and economic goals to overcome these challenges [7]. These involve creating interoperable data protection systems, diversification of data storage systems to reduce geopolitical risks, and encouraging the adoption of secure data processing systems including encryption and anonymization [9]. The incorporation of cross-border data provisions into trade agreements (as in agreements like the TPP can also provide a channel through which a more regulatory alignment can be achieved [1].

8. Conclusion

This paper has discussed how the presence of regulatory inconsistency in cross-border data flows affects the activities and strategic choices of MNEs. Through a qualitative document review method, it has pointed out how disjointed regulatory environments cause compliance costs, decrease the efficiency of operations, and create legal uncertainty. Such issues can be traced to the basis of institutional logics in different jurisdictions, influencing the priorities of regulation and making data governance globally more complicated.

The findings suggest that the question of global practice for data is the ability to balance freedom of data movement with the need to protect privacy, confidentiality, and national interest. While the current regulatory powers are reflective of sensible policymaking, the difference creates an issue in effective global practice. In response, MNEs need to assume diverse approaches in response to the regulatory systems, and policy makers need to be more efficient and coordinated in regulatory approaches to the data.

Finally, these challenges need to be tackled in a multilateral and interdependent manner for the digital economy. International collaboration between governments, international institutions, and the actors in the private sector can build regulatory systems that will encourage innovation and trust. The study can become a part of the existing body of literature on global data regulation by providing information on the interplay between regulatory diversity and firm-level strategies.

9. Future Research

Future research must consider identification of overlaps in the current regulatory regimes and interoperable mechanisms that will reduce fragmentation of cross-border data regulation. With the ongoing development of digital technologies, the issue to consider is whether the current regulatory methods are adaptive and can handle the existing issues. In particular, the studies should examine how paradigms that are customized to traditional data exchanges may be adapted to multi-way flows, which are complex to be supported and that are associated to cloud computing and online communication.

More studies are also needed to draw a better distinction between commercial data flows and data access to government because putting these two issues together may result in too restrictive or misaligned policies. There is also room to consider redistribution of responsibility in the protection of data, especially on areas where prescriptive regulatory models might likely promote formal compliance but not substantive protection.

Lastly, one possible future study would examine how third-party data management services and outsourcing is increasingly playing a role in cross border data governance. The knowledge of these developments in determining regulatory compliance, operational efficiency, and risk management will be invaluable to both firms and policymakers. This type of research would also be very informative in terms of understanding the effects of changing technological and institutional dynamics regarding the future of the global data flows.

10. Policy Implications and Recommendations

10.1. Policy Implications

The results of the current research indicate that coordination and multilateral strategies should be adopted to regulate data across borders. Regulatory fragmentation cannot be effectively dealt with by individual countries or firms on its own but through the concerted efforts of these companies, it is possible to mitigate the inconsistencies and encourage interoperability across jurisdictions. Since all these difficulties are based on the variation in the institutional logic, policymakers need to find a common ground as they attempt to meet the different national priorities.

Among the implications is that there is the need to establish international data mobility frameworks that can address both data mobility, privacy and security concerns. The global institutions can be used to provide multilateral cooperation, which can be used to set standards at the baseline, with local flexibility. Moreover, governments should be receptive to the changing regulatory environments by constantly revising the policies and holding consistent consultations with the involved parties in order to enforce the changes effectively.

The other implication is that trade agreements influence data governance. They can facilitate consistency and ease of doing business globally by putting in place cross-border data provisions in such agreements. However, these frameworks must be carefully designed to avoid reinforcing existing inequalities or limiting policy space for developing economies.

10.2. Recommendations

By keeping up with the implication of the policies, there can be various recommendations to be made in relation to this study that will enhance data governance across borders. First, bilateral and multilateral agreements need to be negotiated on the data protection standards to be harmonized internationally. They should endeavor to minimize regulatory arbitrage while ensuring the appropriate privacy and security protection.

Secondly, there needs to be incentives for accountability and transparency from data custodians. This includes deepening reporting, better monitoring and micro and macro-level sanctions for data misuse and breaches.

Third, governments should have appropriate regulatory frameworks that are both beneficial to data protection and information sharing. This needs to include the technological tools such as encryption and anonymization in its measures, which have the effect of increasing trust but not restricting the data.

Fourth, emerging countries will require help developing the infrastructure and capacity for them to be able to participate in the global data economy. This includes infrastructure development and regulatory capacity and training on digital skills. Lastly, we need to focus more on multi-stakeholder cooperation, such as government, business and international organizations. This can help with the sharing of experience, innovation and make data governance more agile to changes.

Abbreviations

AfCFTA	The African Continental Free Trade Area
EU	The European Union
CCPA	The California Consumer Privacy Act
CLOUD	Clarifying Lawful Overseas Use of Data
CPRA	The California Privacy Rights Act
CSL	Cybersecurity Law
DPA	The Data Protection Act
DSL	The Data Security Law
GDPR	The General Data Protection Regulations
MNEs	Multinational Enterprises
PIPL	Personal Information Protection Law
POPIA	Protection of Personal Information Act
SADC	The Southern African Development Community
TFTA	The Tripartite Free Trade Area
TPP	The Trans-Pacific Partnership
US	The United States

Author Contributions

Amos William Omolo: Conceptualization, Data curation, Formal Analysis, Funding Acquisition, Investigation, Methodology, Resources, Validation, Visualization, Writing – original draft, Writing – review & editing

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] United States Chamber of Commerce and Hunton & Williams LLP, "Business without borders: The importance of cross-border data transfers to global prosperity," 2014. Available: https://www.hunton.com/media/publication/3086_Business_without_Borders.pdf

[2] D. Wood, "Cross-border data transfer: Global data compliance strategies," Duality Tech, Mar. 3, 2024. Available: https://dualitytech.com/blog/cross-border-data-transfer/

[3] K. Rong, Y. Ling, T. Yang, and C. Huang, "Cross-border data transfer: Patterns and discrepancies," *J. Int. Bus. Policy*, 2025, https://doi.org/10.1057/s42214-025-00209-7

[4] F. Sucker and A. Beyleveld, "Cross-border data flows in Africa: Policy considerations for the AfCFTA digital trade protocol," 2022. Available: https://ssrn.com/abstract=4278748

[5] D. A. Kipkoech, "Navigating the crossroads: The challenges of cross-border data flows under domestic laws in Africa," Center for Intellectual Property and Information Technology Law, Nov. 23, 2023. Available: https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/

[6] Center for Intellectual Property and Information Technology Law, "Cross-border data flows in Africa: Exploring legal frameworks and regional importance," 2024. Available: https://cipit.org/wp-content/uploads/2024/11/Cross-Border-Data-Flows-in-Africa-Exploring-Legal-Frameworks-and-Regional-Importance-1_compressed.pdf

[7] Y.-C. Chin and J. Zhao, "Governing cross-border data flows: International trade agreements and their limits," *Laws*, vol. 11, no. 4, p. 63, 2022, https://doi.org/10.3390/laws11040063

[8] N. C. Rotich, "Examining cross-border data flows provisions in Africa's free trade agreements," Center for Intellectual Property and Information Technology Law, Aug. 31, 2023. Available: https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/

[9] GSM Association, "Cross-border data flows: Realizing benefits and removing barriers," 2018. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf

[10] J. Gulia, "Cross-border data transfers : International cooperation and conflicts," *International Journal for Multidisciplinary Research*, vol. 7, no. 2, Apr. 2025, https://doi.org/10.36948/ijfmr.2025.v07i02.41439

[11] E. N. Smirnov, "Directions of development and regulation of cross-border data flows in international trade," *E-Management*, vol. 3, no. 1, pp. 16–26, May 2020, https://doi.org/10.26425/2658-3445-2020-1-16-26

[12] G. Bolatbekkyzy, "Legal issues of cross-border data transfer in the era of digital government," *Journal of Digital Technologies and Law*, vol. 2, no. 2, pp. 286–307, July 2024, https://doi.org/10.21202/jdtl.2024.15

[13] L. Zhao, "The main models of cross-border data transmission regimes: EU, USA and China," *Law and Politics*, no. 4, pp. 50–60, Apr. 2024, https://doi.org/10.7256/2454-0706.2024.4.70797

[14] O. Ismagilova and K. Khadzhi, "Global experience in regulating data protection, transfer and storage," *Economic Policy*, vol. 15, no. 3, pp. 152–175, June 2020, https://doi.org/10.18288/1994-5124-2020-3-152-175

[15] N. Tursunbaeva and A. Abolfazl, "International standards for data protection and cross-border flows," *Bulletin of Science and Practice*, vol. 12, no. 3, pp. 442–448, Mar. 2026, https://doi.org/10.33619/2414-2948/124/50

[16] M. Słok-Wódkowska and J. Mazur, "Between commodification and data protection: Regulatory models governing cross-border information transfers in regional trade agreements," *Leiden Journal of International Law*, vol. 37, no. 1, pp. 111–138, Oct. 2023, https://doi.org/10.1017/s092215652300050x

[17] D. S. Singh and Prerna, "Regulation of cross-border data flow and its privacy in the digital era," *NUJS Journal of Regulatory Studies*, vol. 9, no. 2, May 2024, https://doi.org/10.69953/njrs.v9i2.9