Implementing Data Sovereignty and Digital Privacy in Nigeria Using Legislative Instrument: A Governance and Policy Analysis for a Secure Digital Economy

Destiny Young[1]*, Osinachi Ozocheta[2]

[1]Oil and Gas Free Zones Authority Onne, Rivers State, Nigeria

[2]Stowe School Buckingham, United Kingdom

DOI: https://doi.org/10.51584/IJRIAS.2025.10120028

Received: 19 December 2025; Accepted: 27 December 2025; Published: 05 January 2026

ABSTRACT

This paper provides a detailed governance and policy analysis of Nigeria's legislative instruments deployed to achieve data sovereignty and digital privacy within its rapidly growing digital economy. Nigeria, a key member of the Digital Cooperation Organisation or DCO, utilizes a sophisticated, hybrid regulatory architecture established primarily through the Nigeria Data Protection Regulation 2019 or NDPR and the Data Protection Act 2023 or NDPA (Mitchell & Mishra, 2024). This approach strategically blends comprehensive individual rights protections, largely influenced by the European Union's rights-based model, with stringent, state centric data localisation mandates aimed at economic self reliance and national security (Mitchell & Mishra, 2024; Han, 2024). The core objective is to evaluate how this legislative strategy, using the Governance by Design framework, balances the imperatives of securing national interests and safeguarding data subject rights against the necessity of fostering scalable digital trade (Fedynyshyn, 2025; Mitchell & Mishra, 2024). The analysis finds that Nigeria's reliance on broad geographical restrictions, particularly in critical sectors such as telecommunications and finance, risks functioning as a costly non tariff trade barrier, thereby hindering innovation and exacerbating conflicting legal obligations arising from transnational regimes like the United States CLOUD Act (Han, 2024; Chander, 2025). The study concludes that optimising Nigeria's digital economy necessitates a policy shift from focusing purely on data residency to mandating technical control through measures such as encryption key management and promoting transparent enforcement mechanisms (Thales, 2025; Chander, 2025). This requires leveraging regional initiatives, including the African Continental Free Trade Agreement or AfCFTA, to establish interoperable, trust based data governance frameworks (Mitchell & Mishra, 2024).

Keywords: Data Sovereignty, Cross-Border Data Flows, Data Localisation, Data Governance, Digital Privacy, National Security, Digital Economy

INTRODUCTION

The unprecedented scale and velocity of global data flows have triggered a fundamental reassessment of traditional state authority, culminating in a pervasive political struggle centred on **digital sovereignty** (Kaya & Shahid, 2025; Li, 2025). This dynamic concept is not a static legal definition; rather, it is a contested resource influencing geopolitical strategy and regulatory design across the globe (Ryan, Gürtler, & Bogucki, 2024). Effective governance of the digital economy demands a legislative strategy that carefully reconciles two interdependent objectives: **data sovereignty**, which concerns the legal jurisdiction and policy framework defining who controls the data and where it must legally reside, and **digital privacy**, which focuses on the technical controls necessary to safeguard data during its processing and use (Mitchell & Mishra, 2024; Thales, 2025). Data has transitioned from a mere commodity to a strategic asset integral to national security and economic competitiveness (Li, 2025; Han, 2024).

Nigeria, being one of Africa's fastest growing digital economies and an active member of the Digital Cooperation Organisation or DCO, is a pivotal case study in translating these global principles into domestic legislative action

(Mitchell & Mishra, 2024). The nation has responded to the challenges of transnational data flows by enacting the Nigeria Data Protection Regulation (NDPR) in 2019 and the subsequent Data Protection Act (NDPA) in 2023, formalising its commitment to establishing a secure digital environment (Mitchell & Mishra, 2024). This research seeks to evaluate how Nigeria's hybrid regulatory approach balances its internal claims of control and self reliance with the demands of global interoperability, using a qualitative legal and policy analysis of its core instruments and comparing them against international models.

LITERATURE REVIEW

The academic literature dissects the struggle for control in the digital age, framing it as a conflict between the nonterritorial reality of data and the inherently territorial nature of state authority (Kaya & Shahid, 2025; Hummel et al., 2021).

Defining Digital Sovereignty and Policy Drivers

Digital sovereignty reflects the political struggle for effective control over digital networks, involving elements such as adversarial geopolitics, the multiplicity of state and nonstate actors (multiversity), policy lag (latency), and the use of legislative measures for political objectives (instrumentality and hypocrisy) (Ryan, Gürtler, & Bogucki, 2024). **Data sovereignty**, often seen as a necessary component, asserts the state's highest authority in the realm of data, encompassing independence, autonomy, and exclusivity (Li, 2025). For enterprises, data sovereignty means that legal frameworks define how data may be used, shared, or transferred, binding the information to the laws of the country where it originates or is stored (Fedynyshyn, 2025).

States frequently utilize **data localisation** as the primary legislative instrument to assert this control, legally compelling data to be collected, stored, processed, and routed within domestic borders (Han, 2024; TrustArc, 2025). This practice is justified by governments to enhance national security, protect citizen privacy, and promote domestic digital industrialisation, thereby internalizing the economic benefits (Han, 2024; TrustArc, 2025). However, empirical research often highlights the unintended negative consequences of broad localisation, including reduced national productivity and stifled innovation, leading it to function effectively as a costly **non tariff trade barrier** (Han, 2024; TrustArc, 2025). Furthermore, location does not guarantee protection, as data security ultimately hinges on technical controls like encryption, rather than geography (Thales, 2025; TrustArc, 2025).

The Challenge of Big Tech and Jurisdictional Conflicts

The rise of large technological companies, or **Big Tech firms**, as *de facto* **data sovereigns** significantly complicates traditional state exclusivity over data (Gu, 2023;). These firms determine the true value of data and exert platform power that influences international affairs (Gu, 2023;). Governments regulating this power, such as through the European Union's Digital Markets Act, are engaged in a geopolitical struggle to reassert control over this critical resource (Gu, 2023).

This global effort is complicated by regulatory **fragmentation** and conflicting jurisdictional claims (Kaya & Shahid, 2025; Wan, 2025). The **extraterritorial reach** of instruments like the United States CLOUD Act authorizes US authorities to compel the disclosure of data held by US based providers regardless of its physical location (Chander, 2025; Fedynyshyn, 2025). This directly undermines the sovereignty claims of host nations and contributes to a growing tangle of **regulatory contradictions** and compliance dilemmas (Chander, 2025; TrustArc, 2025).

Theoretical Framework

This analysis employs a theoretical structure that links policy intent with operational reality: the **Tripartite Conceptual Framework** for regulatory design (Mitchell & Mishra, 2024, p. 848) is used to map Nigeria's policies, while **Governance by Design** (Fedynyshyn, 2025) serves as the normative standard for evaluating effective implementation and proposed solutions.

Governance Concept	Abstract Definition	Practical Regulatory Application in Nigeria
Data Residency	Physical storage location	Local hosting mandates in telecoms and government systems
Data Sovereignty	Legal and technical control	Encryption key custody under Nigerian jurisdiction
Data Safeguards	Rights based protection	NDPA data subject rights and adequacy framework
Data Restrictions	Barriers to data flow	Sector specific localisation mandates
Governance by Design	Embedded compliance	RegTech auditing, encryption, access controls

Table 1: Operational Translation of Governance-by-Design Principles in Nigeria

This table summarises the conceptual distinctions underpinning the analysis and illustrates how abstract governance principles translate into operational regulatory tools within Nigeria's digital economy.

The Tripartite Conceptual Framework

This framework categorizes regulatory instruments concerning cross border data flows into three distinct policy areas (Mitchell & Mishra, 2024, p. 848):

1. **Data Enablers** These are policy tools designed to facilitate cross border digital trade, including mechanisms for mutual recognition, interoperability standards, and commitments to prohibit data localisation (Mitchell & Mishra, 2024, p. 848).

2. **Data Safeguards** These encompass the necessary regulatory structures, such as comprehensive data protection laws and independent supervisory authorities, which secure public policy objectives for trusted data flows (Mitchell & Mishra, 2024, p. 850).

3. **Data Restrictions** These involve measures that disproportionately impede cross border data flows, exemplified by overly aggressive or broad data localisation mandates, typically justified by national security or industrial protectionism (Mitchell & Mishra, 2024, p. 853).

Optimized governance facilitates data enablers and enhances safeguards, whilst systematically minimising the application of restrictions (Mitchell & Mishra, 2024, p. 853).

Governance by Design: From Residency to Technical Control

The **Governance by Design** framework mandates embedding regulatory requirements directly into the **technical and operational enforcement mechanisms** that govern data flow (Fedynyshyn, 2025). This approach argues that sovereignty must be maintained not merely through geographical residency, but through **technical control**, such as securing encryption keys and cryptographic means (Chander, 2025; Thales, 2025). This ensures that legal rules are enforceable in practice and reduces exposure to extraterritorial claims, which often undermine purely location-based protections (Fedynyshyn, 2025). Key elements include:

- **Operational Sovereignty:** Ensuring that the systems underpinning sensitive data remain resilient, available, and governed by local authority, incorporating robust business continuity and disaster recovery planning (Fedynyshyn, 2025).

- **Digital Sovereignty:** Focusing on control of the digital assets themselves through auditable workflows and customer managed encryption keys, rather than relying solely on manual oversight (Fedynyshyn, 2025).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

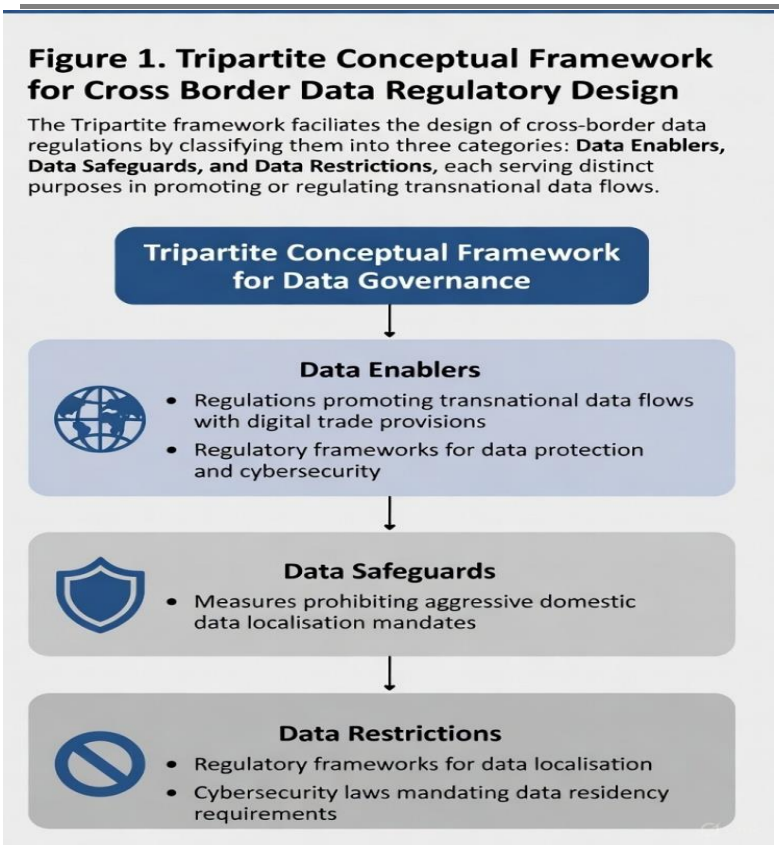

Figure 1: Tripartite Conceptual Framework for Data Governance

This model illustrates the three primary policy areas governments address when formulating regulations for transnational data flows in the digital economy (Mitchell & Mishra, 2024, p. 848). An effective governance approach seeks to maximise enablers and safeguards while minimizing restrictions (Mitchell & Mishra, 2024, p. 853).

Overview of Nigeria's Data Sovereignty and Privacy Landscape

Nigeria's commitment to securing its digital domain is evident in its legal architecture, established through the NDPR in 2019 and the subsequent NDPA in 2023, designed both to protect individual rights (**Data Safeguards**) and assert state control (**Data Restrictions**) (Mitchell & Mishra, 2024).

Legislative Foundations: NDPR 2019 and NDPA 2023

The cornerstone of the regulatory structure began with the **Nigeria Data Protection Regulation 2019**, which set forth essential objectives: safeguarding privacy, ensuring safe transaction conduct, preventing data manipulation, and guaranteeing the global competitiveness of Nigerian enterprises (Mitchell & Mishra, 2024). This framework established comprehensive **data subject rights**, such as the right to data portability, access, deletion, and the right to be forgotten (Mitchell & Mishra, 2024).

The subsequent **Nigeria Data Protection Act 2023** strengthened this foundation by instituting an independent **Data Protection Commission** (Mitchell & Mishra, 2024). The NDPA confirmed the use of an **adequacy framework** for cross border data transfers, allowing data transfer to approved jurisdictions and including alternative safeguards like binding model contracts, thereby aligning Nigeria's standards with international frameworks, such as the EU GDPR (Mitchell & Mishra, 2024, p. 870;).

Asserting Data Sovereignty via Localisation (Data Restrictions)

Nigeria explicitly asserts **data sovereignty**—the state's authority over data characterized by independence and autonomy (Li, 2025)—through mandatory **data localisation mandates** across strategically important sectors, reflecting goals of economic self reliance and national security (Mitchell & Mishra, 2024, p. 871).

1. **Government and Sovereign Data:** All government or sovereign data is mandated to be hosted locally, requiring explicit approval for any offshore hosting (Mitchell & Mishra, 2024, p. 871).

2. **Telecommunications Sector:** All telecommunications companies must host all subscriber and consumer data within Nigeria and are required to peer their internet traffic at a local Nigerian Internet Exchange Point (Mitchell & Mishra, 2024, p. 871).

3. **Financial Services:** Domestic financial transactions processed via Point of Sale or POS must be switched using local services and are explicitly prohibited from being routed outside Nigeria for switching between Nigerian issuers and acquirers (Mitchell & Mishra, 2024, p. 872).

Gaps in Existing Legislative Instruments

Enforcement Capacity and Institutional Constraints

While Nigeria's data protection framework exhibits formal alignment with global best practices, enforcement capacity remains a structural limitation. The establishment of the Data Protection Commission under the NDPA represents an important institutional advancement. However, comparative regulatory studies indicate that newly created supervisory authorities in emerging digital economies often face constraints related to technical expertise, investigative resources, and judicial reinforcement (Chen, 2021).

Effective enforcement depends not only on statutory authority but also on consistent judicial interpretation. At present, Nigeria lacks a substantial body of reported case law clarifying the scope of data subject rights, cross border transfer disputes, or proportionality standards for state access to data. This judicial underdevelopment introduces uncertainty for regulated entities and weakens deterrence effects. Empirical governance research shows that regulatory credibility is significantly enhanced when supervisory decisions are reinforced by predictable judicial review mechanisms (Ryan, Gürtler, and Bogucki, 2024).

Governance-by-design partially mitigates these constraints by shifting enforcement from discretionary oversight toward embedded technical compliance. Automated audit trails, encryption key custody requirements, and continuous compliance monitoring reduce reliance on reactive enforcement and lower institutional burden. This approach is particularly relevant in contexts where regulatory capacity is still consolidating (Fedynyshyn, 2025).

Nigeria's legislative ecosystem is robust in its intent to provide data safeguards and assert digital control, the current framework exhibits critical gaps that challenge the transition from legal theory to secure, operational enforcement.

The most prominent gap is the **high economic cost and administrative burden** imposed by broad data localisation mandates, which fall under the category of **Data Restrictions**

(Han, 2024; TrustArc, 2025). Imposing stringent localisation across critical sectors risks acting as an economically detrimental **non tariff trade barrier**, hindering innovation and curtailing access to the scalable global cloud infrastructure necessary for modern technologies like Artificial Intelligence (Han, 2024; TrustArc, 2025).

A further conceptual gap exists in **confusing data residency with data sovereignty** (Fedynyshyn, 2025; TrustArc, 2025;). Local data residency, or physical storage location, does not guarantee data sovereignty, which depends on legal authority and control, irrespective of where the data resides (Fedynyshyn, 2025). This gap allows the policies to prioritize the state's desire for physical infrastructure control (negative security externality) above optimizing the conditions necessary for competitive market growth (Han, 2024).

Finally, a **pervasive enforcement deficit** is noted in global diagnostic reports, where the adoption of high-level laws (safeguards) often outpaces the development of practical operational and technical enforcement mechanisms (Chen, 2021;).

Comparative International Models

Nigeria's data governance framework constitutes a **hybrid model**, selectively drawing from and reacting to three dominant global regulatory paradigms (Mitchell & Mishra, 2024).

The European Union: Rights Based Paradigm

The EU sets the standard for **rights-based governance** through the **General Data Protection Regulation** or GDPR, guaranteeing comprehensive individual digital rights (Wan, 2025). The GDPR enforces strict rules for data transfers through an **adequacy framework** and mechanisms like Standard Contractual Clauses, ensuring data protection remains in place even during transnational flows (Ryan, Gürtler, & Bogucki, 2024; Wan, 2025). The EU's commitment to protecting individual rights against foreign surveillance has resulted in significant regulatory actions, such as the Schrems II judgment, which found that US surveillance laws undermined the adequacy of data transfers (Ryan, Gürtler, & Bogucki, 2024). Nigeria aligns its data transfer policies and data subject rights with these protective standards (Mitchell & Mishra, 2024).

The United States: Market and National Security Driven Paradigm

The United States traditionally advocates a market driven approach, promoting open data flows (Wan, 2025). However, geopolitical concerns have accelerated a pivot toward a **national security internet**, defined by stringent **digital border controls** aimed at keeping sensitive data *in* (Chander, 2025). This approach is manifested through the **extraterritorial reach** of instruments like the **CLOUD Act**, which compels US based providers to disclose data regardless of its storage location (Chander, 2025; Fedynyshyn, 2025). This assertion of jurisdiction fundamentally conflicts with the sovereignty claims of host nations, generating **jurisdictional overlap** and legal friction (Chander, 2025).

The China Model: State Centric Control

China utilizes a stringent **state centric paradigm**, leveraging laws like the Personal Information Protection Law or PIPL to assert strong sovereign power over data infrastructure (Li, 2025; Wan, 2025). This model emphasizes **mandatory data localisation**, particularly for critical information infrastructure, explicitly linking data control to national security and governance stability (Li, 2025; Wan, 2025). This legislative framework reflects an instrumental purpose, whereby data gathered from businesses may be used to feed and improve state mechanisms, such as the Social Credit System (Chander, 2025). Nigeria's stringent, sector specific localisation mandates share a philosophical alignment with this pursuit of guaranteed state control over strategic data resources (Mitchell & Mishra, 2024, p. 871).

Implementation Challenges

The deployment of Nigeria's hybrid legislative model introduces complexity and geopolitical risk, generating friction points in its implementation.

Jurisdictional Conflict and Sovereignty Erosion

The foremost challenge is the **absolute conflict of laws** created by Nigerian localisation mandates colliding with the **extraterritorial reach** of foreign legal instruments (Chander, 2025; Fedynyshyn, 2025). Compliance with domestic data residency requirements does not grant immunity from compelling disclosure orders issued by foreign governments under statutes like the CLOUD Act (Chander, 2025). This tension undermines the intended legal exclusivity of Nigerian sovereignty, placing multinational organisations in a difficult dilemma and highlighting the pervasive **legal fragmentation** in global governance.

The Costs of Geographic Restrictions

The stringent application of **data restrictions** (localisation) imposes substantial **economic penalties** on businesses operating within Nigeria (Han, 2024; TrustArc, 2025). Empirical evidence demonstrates that compulsory local storage and processing necessitate redundant infrastructure and administrative overhead,

significantly increasing operational costs (TrustArc, 2025). This financial burden disproportionately disadvantages smaller Nigerian enterprises, potentially stalling innovation and functioning as a costly protective trade barrier, thus hindering the digital economy it seeks to secure (Han, 2024).

Risk of Digital Autocracy and Trust Erosion

A key governance risk is ensuring that legislative instruments designed for state control do not inadvertently facilitate **digital authoritarianism** (Chander, 2025). In jurisdictions where national security is strongly prioritized, legislative measures can be utilized to severely limit the right to privacy (Chander, 2025). The reliance on data to manage the state and society, particularly when unchecked, leads to trends toward technical autocracy (Gu, 2023). Maintaining public trust in Nigeria's governance framework is paramount, requiring transparent and proportionate implementation of safeguards to counter any perception of excessive state intrusion (Chander, 2025).

Sectoral Applications of Governance by Design in Nigeria

To operationalise the governance-by-design framework, it is necessary to examine how Nigeria's hybrid data governance model functions within sector-specific regulatory environments. Two sectors are particularly instructive, financial technology and telecommunications, due to their extensive data processing activities and explicit localisation mandates.

Fintech and Payment Systems

Nigeria's fintech sector operates under overlapping regulatory obligations issued by the Central Bank of Nigeria and reinforced by data protection requirements under the NDPA. Domestic switching mandates for Point-of-Sale transactions are intended to preserve transactional sovereignty and reduce foreign dependency. However, governance-by-design principles suggest that sovereignty is more effectively achieved through technical control rather than exclusive geographic routing. In practice, fintech firms increasingly rely on cloud based infrastructure for fraud detection and real time analytics, which challenges strict localisation requirements. Embedding customer managed encryption keys and auditable access controls within payment platforms allows regulators to retain effective oversight without prohibiting cross border computational processing. This approach aligns regulatory intent with operational feasibility and reduces exposure to jurisdictional conflict arising from foreign disclosure laws (Chander, 2025; Fedynyshyn, 2025).

Telecommunications and Subscriber Data

In the telecommunications sector, mandatory local hosting of subscriber data and domestic internet exchange peering are designed to enhance national security and lawful interception capabilities. However, governance-by-design reframes security as a function of system architecture rather than physical location. Telecom operators can embed regulatory controls through encrypted data segmentation, role-based access management, and regulator auditable logging systems. These measures preserve state access and oversight while mitigating risks associated with centralised data concentration. Comparative regulatory analysis indicates that technical enforcement mechanisms are more resilient than geographic mandates when confronting cross border surveillance risks (Han, 2024; Thales, 2025).

Together, these sectoral illustrations demonstrate that governance-by-design enables Nigeria to preserve regulatory authority while reducing the economic and technical inefficiencies associated with rigid localisation policies.

Proposed Legislative and Governance Framework

To secure a resilient digital economy, Nigeria must optimize its legislative instruments by rigorously applying the **Governance by Design** framework, prioritizing verifiable **technical controls** and regional **data enablers** over reliance on restrictive geographical mandates.

Strategic Shift to Technical Control (Governance by Design)

Policy must shift its focus from data location (**residency**) to **technical control** (**digital sovereignty**), as this provides a superior and auditable mechanism for securing data against both unauthorized access and extraterritorial compulsion (Fedynyshyn, 2025; Chander, 2025; Thales, 2025).

1. **Mandate Technical Control (Key Management):** Legislative instruments should mandate that **encryption keys** and cryptographic means remain custodially controlled within Nigeria's legal jurisdiction (Chander, 2025; Thales, 2025). This leverages **cryptographic means** to establish digital territoriality, securing the data irrespective of its physical storage location (Chander, 2025; Thales, 2025).

2. **Privacy Enhancing Technologies (PETs):** The deployment of advanced technologies like **Federated Learning** and **end to end encryption** should be actively promoted within the framework (Thales, 2025). PETs provide a technical mechanism to uphold privacy while enabling the necessary cross border data utilisation for innovation (Thales, 2025).

3. **Operational Sovereignty and RegTech:** The Data Protection Commission should establish standards for **Operational Sovereignty**, requiring organizations to integrate auditable workflows and **regulatory technologies** or RegTech to ensure continuous compliance and resilience against technical failures (Fedynyshyn, 2025).

Institutionalising Ethical Stewardship

The legislative framework must evolve toward institutionalising **ethical stewardship** (Houser & Bagby, 2023). This requires pivoting from viewing data purely as a commodity toward recognizing data as a resource to be governed under public trust (Zygmuntowski, Zoboli, & Nemitz, 2021).

1. **Ethical Stewardship Paradigm:** The framework should mandate an operational code of conduct based on stewardship, ensuring that organizations account for the actual impact of data use on data subjects and prioritize their welfare above mere compliance (Houser & Bagby, 2023).

2. **Public Data Commons:** Nigeria should explore legal interventions, such as the creation of **Public Data Commons**, to manage informational resources for broad public benefit, integrating individual rights and inclusive deliberation into data allocation decisions (Zygmuntowski, Zoboli, & Nemitz, 2021).

POLICY RECOMMENDATIONS

To optimize Nigeria's framework for secure digital governance, recommendations are focused on enhancing data enablers and restructuring restrictions based on the Governance by Design philosophy.

1. **Refining Localisation through Specificity (Minimising Restrictions):** Mandatory localisation mandates must be **narrowly defined** and applied exclusively where demonstrably essential, such as securing core sovereign government infrastructure (Han, 2024; Mitchell & Mishra, 2024, p. 897). When alternatives using advanced technical controls are available, these must be prioritized over broad geographical restrictions to minimize economic friction (Han, 2024; TrustArc, 2025).

2. **Strengthening Independent Enforcement (Improving Safeguards):** The Data Protection Commission must be fully empowered as an **independent supervisory authority** (Mitchell & Mishra, 2024, p. 894;). It must prioritize enforcement clarity, establishing transparent criteria for adequacy determinations for cross border transfers and leveraging international engagement, perhaps through the Global Privacy Assembly, to acquire sophisticated regulatory expertise (Mitchell & Mishra, 2024, p. 894).

3. **Fostering Regional Harmonisation (Facilitating Enablers):** Nigeria should aggressively leverage its participation in **ECOWAS** and the **African Continental Free Trade Agreement** or AfCFTA to promote the development of **mutual recognition mechanisms** for data protection standards (Mitchell & Mishra,

2024, p. 890). This creates trust based regional governance frameworks, reducing the incentives for costly unilateral restrictions (Mitchell & Mishra, 2024, p. 890).

4. **Implementing Portability and Interoperability (Facilitating Enablers):** Urgent policy attention is required to enforce robust standards for **data interoperability and portability** (Mitchell & Mishra, 2024, p. 893; Chen, 2021). These technical standards empower data subjects and cultivate a more competitive digital ecosystem by simplifying data exchange (Chen, 2021).

CONCLUSION

Nigeria has enacted sophisticated legislative instruments to pursue its goals of **data sovereignty** and **digital privacy**, adopting a hybrid governance model that blends rights-based safeguards with protective localisation mandates (Mitchell & Mishra, 2024). This strategic approach positions Nigeria as a key actor in African digital governance.

However, analysis confirms that the current reliance on geographical restrictions risks imposing significant economic penalties, constraining innovation, and undermining competitiveness (Han, 2024; TrustArc, 2025). Moreover, the exposure to **jurisdictional conflicts** with powerful extraterritorial regimes, such as the United States CLOUD Act, exposes the limitations of relying on purely territorial definitions of control (Chander, 2025; Fedynyshyn, 2025).

A resilient and secure digital economy for Nigeria requires legislative policy to pivot toward the **Governance by Design** framework, prioritizing verifiable **technical controls**—such as encryption and key management—over mandates concerning data residency (Thales, 2025; Chander, 2025). By strengthening independent enforcement, embracing principles of ethical stewardship, and leading regional harmonisation efforts through ECOWAS and AfCFTA, Nigeria can successfully assert its national interests while securing a competitive digital future.

REFERENCES

1. Chander, A. (2025). The national security internet. Scholarship at Georgetown Law. Retrieved April 7, 2025, from https://scholarship.law.georgetown.edu/
2. Chen, R. (2021). Mapping data governance legal frameworks around the world, findings from the global data regulation diagnostic (Policy Research Working Paper 9615). World Bank.
3. Fedynyshyn, R. (2025, September 23). Data sovereignty, what does compliance require in 2026? N iX. Retrieved November 18, 2025, from https://www.n-ix.com/data-sovereignty/
4. Gu, H. (2023). Data, big tech, and the new concept of sovereignty. Journal of Chinese Political Science, 29(4), 591 to 612.
5. Han, S. (2024). Data and statecraft, why and how states localise data. Business and Politics, 26(2), 263 to 288.
6. Houser, K. A., and Bagby, J. W. (2023). Next generation data governance. Duke Law and Technology Review, 21(1), 62 to 106.
7. Hummel, P., Braun, M., Tretter, M., and Dabrock, P. (2021). Data sovereignty, a review. Big Data and Society, 8(1), 1 to 17.
8. Kaya, M., and Shahid, H. (2025). Cross border data flows and digital sovereignty, legal dilemmas in transnational governance. Interdisciplinary Studies in Society, Law, and Politics, 4(2), 219 to 233.
9. Li, L. (2025). Data sovereignty and national security, governance challenges and pathways in the digital age. Global Review of Humanities, Arts, and Society, 1(1), 49 to 58.
10. Mitchell, A. D., and Mishra, N. (2024). Cross border data regulatory frameworks, opportunities, challenges, and a future forward agenda. Fordham Intellectual Property, Media and Entertainment Law Journal, 34(4), 842 to 899.
11. Ryan, M., Gürtler, P., and Bogucki, A. (2024). Will the real data sovereign please stand up, an EU policy response to sovereignty in data spaces. International Journal of Law and Information Technology, 32, eaae006.

12. Thales. (2025, June 10). Why data sovereignty and privacy matter to you, not just nations. Retrieved August 3, 2025, from https://cpl.thalesgroup.com/blog/encryption/data-sovereignty-privacy-governance
13. TrustArc. (2025). The global rise of data localisation, risks, tradeoffs, and what comes next. Retrieved October 26, 2025, from https://trustarc.com/resource/global-rise-data-localization-risks/
14. Wan, Y. (2025). The regulatory framework, practical challenges, and solution pathways for cross border data flow. International Theory and Practice in Humanities and Social Sciences, 2(5), 47 to 58.
15. Zygmuntowski, J. J., Zoboli, L., and Nemitz, P. F. (2021). Embedding European values in data governance, a case for public data commons. Internet Policy Review, 10(3).