Journal of Basics and Applied Sciences Research (JOBASR)
ISSN (print): 3026-9091, ISSN (online): 1597-9962
Volume 4(2) March 2026
DOI: https://dx.doi.org/10.4314/jobasr.v4i2.23

Data Sovereignty and The Leaky Pipe: Charting A Course for Data Governance and Information Security in Nigeria and Africa

Yahya Umar Muhammad[1*], Ibrahim Abubakar[2], & Eli Adama Jiya[3]
[1]Department of General Studies, Katsina State College of Health Sciences and Technology, Katsina
[2]Department of Computer Science, Federal University, Gusau
[3]Department of Information and Technology, Federal University, Dutsinma.
[*]Corresponding Author Email: **abdurrashidnasir@gmail.com**

ABSTRACT
The enactment of the Nigeria Data Protection Act (NDPA) 2023 marks a significant milestone in Africa's pursuit of digital sovereignty. However, the presence of strong legislation does not automatically guarantee effective data protection in practice. This study aims to examine the pressure between Nigeria's evolving data protection framework and the real-world challenges of information security, aiming to determine whether legislative progress alone can achieve meaningful data sovereignty and whether institutional, technical, and infrastructural capacities are equally important. To achieve this, the study adopts a qualitative doctrinal legal analysis of the Malabo Convention and the Nigeria Data Protection Act (NDPA) 2023, combined with a thematic review of peer-reviewed articles, institutional reports, and industry publications from 2020-2026. Data were synthesized narratively to identify patterns, challenges, and actionable recommendations. The study finds that the NDPA 2023 marks a significant milestone, aligning Nigeria with global data protection standards. However, implementation remains constrained by weak enforcement, institutional capacity gaps, a shortage of skilled professionals, inadequate infrastructure, and dependency on foreign-owned cloud services. Key friction points include the tension between legal authority and technical capacity, disproportionate compliance burdens on SMEs, and erosion of public trust due to inconsistent enforcement. It concludes that transitioning from a passive data colony to a digital powerhouse requires sustained investment in people, institutions, and infrastructure to ensure effective implementation and enforcement of data protection laws. The study contributes theoretically by integrating legal, security, and implementation science perspectives on the data governance gap, and practically by offering a policy framework with lessons for Africa.

Keywords:
Data Governance,
Nigeria Data Protection Act (NDPA),
Information Security,
Data Sovereignty,
Cybersecurity.

INTRODUCTION

Africa is frequently characterized as a "leapfrog" continent because many countries in the region have bypassed landline telephones in favor of mobile phones and traditional banking systems in favor of mobile banking **(Aker & Cariolle, 2023).** The shift to mobile devices for internet access has fundamentally changed how data is generated across the continent. Simple daily activities such as transferring money via mobile apps, chatting on social platforms, and using digital services now produce a vast volume of data (Kwet, 2020). **D**espite these developments, an important issue remains unresolved i.e., the governance and protection of this rapidly growing pool of digital data.

For decades, African user data has predominantly been controlled by big technology companies located outside of Africa (Sun et al., 2025). This situation has generated increasing concern among scholars and policymakers about what is commonly described as "digital colonialism" or "data colonialism" (Raji et al., 2025), a process through which data produced in developing regions becomes a resource that fuels technological innovation and economic value elsewhere, enabled by the control of critical digital infrastructure by foreign entities (Salami, 2024). These concerns have contributed to a growing continental push for data sovereignty, as African governments seek greater control over how data generated within their jurisdictions is collected,

How to cite this article: Yahya U. M., Ibrahim A., & Eli A. J. (2026). Data Sovereignty and The Leaky Pipe: Charting A Course for Data Governance and Information Security in Nigeria and Africa. *Journal of Basics and Applied Sciences Research*, *4*(2), 224-232. https://dx.doi.org/10.4314/jobasr.v4i2.23

processed, and protected (Ajuna, 2025). Recent developments show significant regulatory momentum across the continent. The Pan-African Parliament has called for Africa to assert full sovereignty over its sensitive digital data and is also developing a legal frame works for cybersecurity and artificial intelligence governance (Pan-African Parliament, 2026).

According to Juma & Faturoti (2025), "as of January 2024, 36 of the 55 African Union (AU) member states (65%) have enacted comprehensive data protection laws. Significantly, one-third of all data protection laws in Africa have been passed within the last five years, signaling a rapid acceleration in legislative activity". However, researchers such as Ajuna (2025), point out that, passing legislation doesn't automatically translate into effective data protection in practice. The real challenge, she argues, comes down to practical realities such as weak institutions, insufficient skilled personnel, and cybersecurity systems that are inadequate to address emerging threats. Without those things, even the best laws on paper may have limited impact.

Despite this increase in data protection laws across Africa and the enactment of the Nigeria Data Protection Act 2023 in particular, a significant gap continues between legal frameworks and the practical ability to implement them effectively. Although researchers have documented this governance gap, there is limited systematic analysis of how Nigeria, as Africa's largest economy, deals with the tension between affirming legal authority over data and developing the institutional, technical, and infrastructural capacity to secure it. This gap is particularly critical given the country's digital transformation path, its reliance on foreign-owned digital infrastructure, and its vulnerability to cyber threats. In view of this, Nigeria, as the largest economy in Africa, serves as a test case for whether African countries can actually build data governance frameworks and security capacity at the same time. This article therefore, aims to examine how Nigeria is trying to claim legal authority over its data while also developing the tools to protect it with a focus on identifying existing gaps and proposing actionable solutions.

This study aims to: (1) examine the evolution of Nigeria's data protection framework from the NDPR 2019 to the NDPA 2023 and how it aligns with continental and global standards; (2) identify the technical, institutional, and infrastructural challenges that hinder effective data protection in Nigeria; (3) analyze the friction points between legal sovereignty and practical security capacity in Nigeria's digital ecosystem; and (4) propose a context-sensitive framework to strengthen Nigeria's technical sovereignty. Accordingly, this study is guided by four research questions: (1) How has Nigeria's data protection framework evolved, and how does it align with continental and global standards? (2) What technical, institutional, and infrastructural challenges hinder effective data protection implementation in Nigeria? (3) What friction points emerge between Nigeria's legal sovereignty and its practical security capacity? (4) What strategies can enhance Nigeria's technical sovereignty?

The study offers a systematic analysis of Nigeria's data protection implementation gap, integrating legal, security, and implementation science perspectives. It provides policy recommendations for strengthening Nigeria's technical sovereignty, with lessons applicable across Africa.

The study employs a qualitative design combining doctrinal legal analysis of the Malabo Convention and NDPA 2023 with a thematic review of secondary sources (2020–2026). Findings were synthesized narratively to identify patterns, challenges, and actionable recommendations.

MATERIALS AND METHODS

This study adopts a doctrinal legal analysis approach along with a qualitative review of secondary sources to examine the relationship between legal frameworks and practical information security outcomes**.** Primary sources include the African Union's Malabo Convention (2014) and the Nigeria Data Protection Act (NDPA) 2023. The qualitative content analysis technique systematically reviews and synthesizes the selected materials. Sources were selected based on relevance, recentness, and credibility, while efforts were made to ensure consistency and reliability in the interpretation of legal and policy documents.

- **Search Strategy**: A systematic search was conducted across PubMed, IEEE Xplore, Scopus, Google Scholar, and African Journals Online (AJOL) for publications from 2020-2026. Keywords included "data protection," "NDPA," "cybersecurity," "digital sovereignty," and related terms.

- **Inclusion Criteria:** Studies were included if they addressed data protection or cybersecurity in Nigeria or Africa; were peer-reviewed articles, institutional reports, or reputable industry publications; and were in English. Opinion pieces and duplicates were excluded.

- **Analytical Framework:** Data were extracted on legal provisions, institutional roles, infrastructure challenges, and implementation barriers. Thematic analysis was used to identify patterns, with findings synthesized narratively.

Limitations: This study relies on secondary sources, which may introduce publication bias. The English-only search may exclude relevant non-English publications, and the Nigeria-specific focus limits generalizability.

RESULTS AND DISCUSSION

The analysis reveals a complex interplay between continental aspirations and the realities of national implementation in Nigeria's data governance landscape.

At the continental level, the African Union has advanced normative frameworks, including the Malabo Convention (2014) and the AU Digital Transformation Strategy (2020–2030) (African Union Commission, 2025). However, implementation remains uneven, with only 16 of 55 member states having ratified the Malabo Convention and enforcement capacity varying widely (Juma & Faturoti, 2025).

At the national level, Nigeria's transition from the NDPR 2019 to the NDPA 2023 represents significant legislative progress, establishing a comprehensive legal framework and creating the Nigeria Data Protection Commission (Federal Republic of Nigeria, 2023). Yet persistent implementation gaps remain: enforcement is inconsistent, hindered by limited institutional capacity, fragmented regulation, and low public awareness (Juma & Faturoti, 2025). Additionally, structural dependencies on foreign-owned digital infrastructure complicate regulatory oversight and undermine practical enforcement (Ilehomon, 2025).

These findings highlight a critical tension: while Nigeria has established strong legal authority over its data, the technical and institutional capacity to operationalize that authority remains underdeveloped. This gap is what forms the central friction point examine below.

The Emerging Regulatory Framework: From Malabo to Lagos

The push for African data governance operates on two interconnected levels: continental initiatives aimed at harmonizing regulatory standards across the region and national efforts that translate these frameworks into domestic law and institutional practice (African Union Commission, 2025; Raji et al., 2025).

- **The Continental Vision: The Malabo Convention:** At the continental level, the African Union has sought to harmonize digital governance through the Malabo Convention. Adopted in 2014, this framework addresses three interconnected challenges: regulating electronic commerce, safeguarding personal data, and establishing common standards for addressing cybercrime (African Union, 2014). The convention aims to provide member states with a harmonized legal structure capable of supporting the region's rapidly expanding digital economy (African Union, 2014; Gakiria & Gitonga, 2025).

  However, the implementation of the convention has been slow. It took nearly a decade for the agreement to enter into force in 2023, reflecting the broader challenges of achieving policy coordination across diverse African political and legal systems (Diallo, 2024). As a result, while the convention represents an important symbolic commitment to digital governance, its practical impact remains limited until its provisions are more widely incorporated into national legislation (Gakiria & Gitonga, 2025). This finding highlights a gap between continental policy ambition and practical implementation across member states. Juma & Faturoti (2025) report that, to complement this framework, the African Union's Digital Transformation Strategy (2020–2030) calls for harmonized legal and institutional measures to protect personal data and privacy rights. Yet, in practice, enforcement remains inconsistent, hindered by limited capacity, fragmented regulation, and low public awareness.
- The National Level: Nigeria’s Data Protection Framework**:** At the national level, the continental push for data governance is taking shape through domestic laws and regulations. Nigeria, as Obi (2020) observes, illustrates this trend well. For much of the past decade, the country’s data protection landscape rested on the Nigeria Data Protection Regulation (NDPR) 2019, issued by the National Information Technology Development Agency. While the NDPR marked a significant early effort, it was widely understood as a regulatory instrument rather than a comprehensive legislative framework (Modilim et al., 2024).

  This changed when the Federal Government of Nigeria enacted the Nigeria Data Protection Act 2023. The Act provides a comprehensive legal foundation for safeguarding personal data, reinforces the privacy rights of Nigerian citizens, and establishes the Nigeria Data Protection Commission as an independent authority tasked with overseeing compliance and enforcement (Federal Republic of Nigeria, 2023). This represents a major institutional and legal advancement in Nigeria’s data governance architecture. (Modilim et al., 2024; Juma & Faturoti, 2025).
- **Key Provisions of the Nigeria Data Protection Act:** The Nigeria Data Protection Act 2023 establishes a comprehensive framework for the governance of personal information. It mandates that data processing be fair, lawful, and transparent, and imposes a clear duty on

organizations to implement appropriate security measures. The Act also restricts cross-border data transfers, allowing them only when adequate safeguards exist, an approach similar to the GDPR, but shaped to fit Nigeria's own context (Iloba, 2025). However, the challenge, as Juma and Faturoti (2025) point out, is that legislative progress has not yet translated into full implementation. Enforcement remains uneven, hindered by limited capacity, fragmented regulation, and low public awareness. Nonetheless, the Act signals a decisive move away from voluntary compliance toward a binding, rights-respecting model of data protection.

The Legal Sovereignty

Although the adoption of modern data protection laws across Africa represents an important step toward strengthening digital sovereignty, the presence of legislation alone does not guarantee effective protection of personal data (Juma and Faturoti, 2025). In many emerging digital economies, there's often exists a gap between passing new regulations and actually having the tools and institutions to put them into practice (Cenfri, 2025). Juma & Faturoti (2025), argued that data protection is about more than legislation. Without solid institutions, skilled technical teams, and proper cybersecurity infrastructure, even the best laws struggle to deliver real results.

Nigeria took a major step forward with the passage of the Nigeria Data Protection Act 2023. The law sets out clear rules for organizations that collect and handle personal data, while also strengthening the rights of individuals over how their information is used. It also established the Nigeria Data Protection Commission as the main regulatory body responsible for overseeing compliance and enforcing the law (Nwodo & Amucheazi, 2025). With these legislative developments aligning, Nigeria is now closer to global standards for data protection (Juma & Faturoti, 2025). Still, as the same researchers caution, the legal alignment with global standards alone is not enough; the real issue lies in their enforcement. They argue that even the most ambitious legislation can be undermined by weak enforcement, limited autonomy of regulators, and the absence of meaningful redress mechanisms**.**

Challenges with the Technical Sovereignty

While the NDPA sets the legal standard, translating data sovereignty into reality requires more than legislation. This section looks at four interrelated issues that limit Nigeria's ability to exercise significant control over its digital assets: inadequate infrastructure, inadequate human capital, the scope of cybercrime, and the digital divide.

- **Inadequate Infrastructure:** Inadequate infrastructure is one of the fundamental obstacles that Nigeria faces in the pursuit of technical sovereignty. According to Ikechukwu Nnamani, CEO of Digital Realty Nigeria, "there's no data center in Nigeria that is AI-ready" (The Sun, 2025). According to another expert, Chidozie Managwu, an AI governance advocate, warned that Nigeria's National AI Strategy, launched in April 2025 to position the country as a West African AI hub, will remain aspirational without investment in sovereign data infrastructure. "We cannot be a hub without the backbone to support it," he said, cautioning that AI policies without infrastructure would only deepen Nigeria's dependence on foreign technology platforms (Tribune, 2025).
- **Inadequate Human Capital:** Beyond infrastructure shortfalls, Nigeria's pursuit of technical sovereignty faces a more major constraint, i.e., inadequate human capital. According to a research report by Marthaler (2025), "the country's cybersecurity workforce stands at approximately 45,000 professionals as of 2024, representing just 2.8% of the broader technology sector employment base." According to Deloitte's Cybersecurity Outlook 2025, 67% of global organizations—including those in Nigeria—operate below the required cybersecurity headcount. Experts note that this gap is worsened by the exodus of Nigerian professionals seeking better opportunities abroad, leaving firms unable to prevent or recover from breaches (Omotayo, 2025).
- **The Rise and Scope of Cybercrime:** Nigeria is among the top five nations in the world for cybercrime exposure, with attacks increasing at an exponential rate, according to cybersecurity researcher Isaac Adinoyi Salami of the University of Tampa's Center for Cybersecurity. He emphasized that as growing fraud jeopardizes financial stability, public confidence, and economic resilience, cybersecurity is no longer only a financial-sector issue but also a priority for citizen protection linked to national stability (Iwedike, 2025).
- **The Digital Divide:** Nigeria's pursuit of technical sovereignty is undermined by a stark digital divide. While mobile broadband has expanded rapidly, connectivity remains deeply unequal. Umeh (2025) reports that only 23 percent of rural communities have internet access compared to 57 percent in urban areas-a gap that the NCC warns continues to widen. Dr. Aminu Maida, the Commission's Executive Vice Chairman, warned that "the lack of

connectivity in rural areas is not just a development issue but a national security concern" (Umeh, 2025).

The Friction Points in Nigeria's Data Governance

The gap between Nigeria's data governance framework and its **implementation** creates three friction points: **Legal Authority vs. Technical Ability, Regulatory Burden on SMEs, and the Gap in the Enforcement**

- **Legal Authority vs. Technical Ability:** The NDPA gives Nigeria strong legislative authority, but the country's technical ability to put it into practice is still severely lacking. Juma and Faturoti (2025) emphasize that while Nigeria's legal framework exhibits ambition and alignment with global best practices, "the real test lies in enforcement." They caution that even ambitious legislation can be undermined by weak enforcement, limited regulatory autonomy, and the absence of redress mechanisms. They also note that the NDPC faces institutional constraints that impede its ability to investigate breaches, impose sanctions, or provide accessible redress to citizens (Juma & Faturoti, 2025).
- **Regulatory Burden on SMEs:** Studies reveal that small to medium enterprises (SMEs) face difficulties in complying with data protection regulations due to a lack of capacity and knowledge (Kasali et al., 2025). Peer-reviewed research confirms this finding, revealing that "most lacked even basic awareness of the NDPR, let alone the capacity for full compliance, primarily due to limited financial and human resources" (Femi, Adenomon, Aimufua & Ibrahim, 2025). As David Idris, CEO of Glemad, explains, "SMEs face a unique challenge; they must embrace AI and automation to remain competitive, yet many lack the resources to implement full-scale compliance infrastructures" (Punch Newspapers, 2025). While some experts argue compliance builds trust and attracts investment, the immediate reality for cash-strapped SMEs is that compliance costs compete directly with product development and growth initiatives (Kasali et al., 2025).
- **The Enforcement Gap:** Although the Nigeria Data Protection Act 2023 was passed, its enforcement remains less effective than in the country compared to similar African countries. Juma and Faturoti (2025) discovered that while Kenya has made significant strides in the enforcement of data protection laws, Nigeria still faces fundamental problems due to a lack of institutional capacity, fragmented regulations, and poor public awareness. Although the NDPA offers a solid framework, Friday Odeh, Country Director of Accountability Lab Nigeria, noted that for it to be effective, strong execution and public awareness are necessary. Without them, breaches involving personal data often go unreported, leaving citizens open to exploitation (Oweh, 2025). According to Juma and Faturoti (2025), this enforcement gap discourages security spending, thereby increasing vulnerability to cybercrime.

The Way Forward: Building Nigeria's Technical Sovereignty

Establishing a sustainable future demands that Nigeria go beyond just changing laws and make strategic investments in the human resources and institutional abilities necessary to fill crucial gaps in skills, education, and professional growth.

1. **Capacity Building as National Security:** It would take consistent investment in human resources to close Nigeria's technical sovereignty gap. Kareem (2025) reports that the Director-General of NITDA referred to people as "the technology component of any innovation ecosystem," highlighting the importance of workforce development for the country's digital transformation. To bridge this gap, coordinated efforts are needed across three key areas:
    - **University Curriculum Reform:** Reforming the educational curriculum will play a vital role in bridging the capacity gap. Ramezan (2023) found that university-industry collaboration improves students' cybersecurity readiness by exposing them to real-world threats and professional standards, bridging the gap between theory and practice to produce more employable graduates.
    - **Public-Private Training Initiatives:** Government-funded training programs can rapidly boost cybersecurity skills and strengthen national defenses. Examples like the Federal Ministry of Education's Cyber 30-30 project, which awarded ISC2 certifications to 418 young Nigerians, and the NITDA/Cisco partnership, offering free cybersecurity courses, illustrate the success of this strategy (Tribune Online, 2024; The Guardian Nigeria, 2025). These initiatives highlight the importance of maintaining ongoing public-private cooperation as a key part of Nigeria's efforts to build cybersecurity capacity.

- **Talent Retention Programs:** Docquier & Rapoport (2012), in their study, indicate that providing incentives such as competitive remuneration, research funding, and innovation hubs for skilled professionals can mitigate the migration of skilled cybersecurity professionals to stay and work in Nigeria rather than moving abroad, a phenomenon called "brain drain".

2. **Securing the Data Locally:** Nigeria currently lacks data sovereignty, with sensitive information stored on foreign platforms, a dependency that exposes the nation to external surveillance and influence, according to NITDA's Director-General (Anthony, 2025). Unitellas Edge Cloud CEO Smith Osemeke warned that foreign hosting leaves Nigeria "vulnerable to external breaches, data manipulation, and loss of digital sovereignty" (Salami, 2025). Consequently, experts emphasize that storing data within the country is essential to safeguarding national sovereignty (Salami, 2025).
3. **Context-Aware Security Models:** Kshetri (2025) contends that cybersecurity frameworks in nations like Nigeria must be adapted to local socio-technical realities rather than relying solely on Western models. This requires accounting for how Nigerians connect to the internet, the threats they encounter, the languages they speak, and the diverse needs of different business categories.
    - **Mobile-First Security:** In Nigeria today, wireless broadband, especially mobile internet has become the main way Nigerians get access to the internet, serving as the main connectivity in both rural and urban areas (Bahia et al., 2020). Therefore, Smartphones and other mobile devices must be given priority in security designs.
    - **Local Language Phishing Awareness:** Combating phishing and social engineering assaults, which continue to be among the most prevalent cyber threats globally, requires crafting messages in languages that people can comprehend. (The Guardian Nigeria, 2025). Therefore, Local languages, including Hausa, Yoruba, Igbo, and Pidgin, should be used in public cybersecurity campaigns (Cybersafe Foundation, 2025).
    - **Resilience Against Local Threats:** According to Chrisos (2025), although cyber threats may cross national boundaries, their nature is significantly influenced by geography. Attackers' tactics and defenders' responses are influenced by economic factors, regulatory frameworks, and cultural background. This discovery highlights a crucial realization for cybersecurity strategy: companies need to embrace location-sensitive tactics that are purposely adopted to local threats, legislation, and realities, rather than generic approaches.

A Risk-Based Approach for SMEs: for this, the NDPC should implement a tiered compliance system where large organizations like banks undergo full audits, while micro-businesses with minimal data processing follow simplified, low-cost rules. Such risk-based models are globally recommended because they reduce regulatory burden without compromising protection (Kuner, 2020).

CONCLUSION

This study examined Nigeria's journey toward data sovereignty, focusing on the evolution of its data protection framework, implementation challenges, and strategies for strengthening technical sovereignty. The findings reveal that while Nigeria has made significant legislative progress, evolving from the NDPR 2019 to the NDPA 2023. A persistent gap remains between legal frameworks and practical implementation. Africa is no longer merely a passive supplier of data for the global digital economy, as shown by the passage of the Nigeria Data Protection Act (NDPA) 2023. However, having a law on paper is different from ensuring security in practice. Nigeria must bridge the gap between the legal framework (boardroom) and the technical implementation (server room) to fully unlock the potential of its data. Building public trust requires consistent and effective enforcement, investing in skilled personnel and technological infrastructure, and creating security architectures that can withstand both local and global cyber threats. This study provides a systematic analysis of Nigeria's implementation gap, an underexplored area, offering policy recommendations with continental relevance, while limitations in secondary data and scope highlight the need for future empirical and comparative research across Africa. Transitioning from a data colony to a digital powerhouse will take time, but Nigeria and Africa as a whole can set their own standards and shape their digital future if they are dedicated to

developing local capacity aligning governance frameworks with practical implementation realities. This study therefore underscores the need for an integrated approach that combines legal reforms, institutional strengthening, and technical capacity development as a pathway to achieving sustainable data sovereignty.

REFERENCE

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention). https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union Commission. (2025, December 2). *AU Commences Validation of Data Governance Frameworks to Accelerate Digital Single Market by 2030*. African Union.

https://au.int/en/pressreleases/20251202/validation-data-governance-frameworks-accelerate-digital-single-market

Ajuna, D. (2025). *Beyond the GDPR: Culturally-Contextualized Privacy and Data Protection in Africa's Expanding Digital Landscape* (Publication No. [if available]) [Doctoral dissertation, University of Ottawa]. uO Research. http://hdl.handle.net/10393/51067

Aker, J. C., & Cariolle, J. (2023). *Mobile Phones and Development in Africa: Does the Evidence Meet the Hype?* Palgrave Macmillan. DOI:10.1007/978-3-031-41885-3

Anthony, U. A. (2025, September 2). *Federal Government Set to Partner with Tech Firms for Hyperscale Data Centres*. *Independent Newspaper Nigeria*. https://independent.ng/federal-government-set-to-partner-with-tech-firms-for-hyperscale-data-centres/

Bahia, K., Castells, P., Cruz, G., Masaki, T., Pedrós, X., Pfutze, T., Rodriguez-Castelan, C., & Winkler, H. (2020). *The Welfare Effects of Mobile Broadband Internet: Evidence from Nigeria* (IZA Discussion Paper No. 13219). Institute of Labor Economics (IZA). https://www.iza.org/publications/dp13219

Cenfri. (2025, August 8). *Financial Sector Regulation in the Digital Economy: Priorities for Emerging Markets*. https://cenfri.org/articles/financial-sector-regulation-in-the-digitial-economy-priorities-for-emerging-markets/

Chrisos M. (2025). *One World, Many Threats: How Regional Realities Shape Global Cyber defense*. Anomali Blog. https://www.anomali.com/blog/one-world-many-threats-how-regional-realities-shape-global-cyber-defense

Cybersafe Foundation. (2025). *Confam Am Again Campaign*. https://cybersafefoundation.org/past-programs/confam-am-again-campaign/

Diallo, B. (2024). Entry into force of the Malabo Convention: Challenges and Issues Related to Cybersecurity and Personal Data Protection in Africa. *Global Africa*, (5). https://www.globalafricasciences.org/issue-05

Docquier, F., & Rapoport, H. (2012). Globalization, Brain Drain, and Development. *Journal of Economic Literature*, *50*(3), 681–730. https://doi.org/10.1257/jel.50.3.681

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

Femi, A. G., Adenomon, M. O., Aimufua, G. I. O., & Ibrahim, U. (2025). Evaluating the Level of Compliance with the Nigeria Data Protection Regulation (NDPR): Insights from Organizations Across Key Sectors. *Journal of Cyber Security*, *7*, 377–394. https://doi.org/10.32604/jcs.2025.069185

Gakiria, A., & Gitonga, T. M. (2025, January 29). *What is the Malabo convention?* DiploFoundation. https://www.diplomacy.edu/blog/what-is-the-malabo-convention/

Iloba, A. (2025). Data Privacy and Consumer Protection in Nigeria's Digital Economy: A Legal Examination of the Nigeria Data Protection Act, 2023. *Zenodo*. https://doi.org/10.5281/zenodo.17055818

Iwedike, P. (2025, May 14). Cybersecurity and Citizen Protection in 2025: Safeguarding Nigeria's Digital Future. *The Guardian Nigeria*. https://guardian.ng/opinion/cybersecurity-and-citizen-protection-in-2025-safeguarding-nigerias-digital-future/

Juma, I., & Faturoti, B. (2025). Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice. *International Review of Law, Computers & Technology*, 1–25. https://doi.org/10.1080/13600869.2025.2506918

Kareem, A. (2025, October 22). *NITDA, Cisco Open Application for Cybersecurity Training*. *The Guardian Nigeria*. https://guardian.ng/news/nitda-cisco-open-application-for-cybersecurity-training/

Kasali, K., Toriola, G. O., Alarape, B. Y., Omosunlade, A., & Deborah, E. N. (2025). Trust-

Centered Digital HR Transformation in Nigeria: Integrated Framework for Ethics, Data Privacy and Workplace Inclusion. *International Journal of Research in Human Resource Management, 7*(2), 746–756. https://doi.org/10.33545/26633213.2025.v7.i2g.397

Kshetri, N. (2021). Cybersecurity Management in Developing Economies. IT Professional, 23(2), 54–60. https://doi.org/10.1109/MITP.2020.3042131

Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford University Press.

Kwet, M. (2020). Digital Colonialism: The Role of Global Tech Companies in African Mobile Infrastructure. *Surveillance & Society*, 18(2), 145-163.

Marthaler, F. (2025, November 5). Nigeria Top 30 Trending Roles in the Cybersecurity & Digital Trust Industry: Strategic Workforce Planning, Hiring Trends, In Demand Skillsets, Demand Push, Salary Benchmarking, Job Demand and Supply : 2025 Edition. *Talenbrium*. https://www.talenbrium.com/report/nigeria-top-30-trending-roles-in-the-cybersecurity-digital-trust-industry

Modilim, S. N., Bolarinwa, I., Omidiora, M. T., & Tawo, O. (2024). Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment. *International Journal of Law Management and Humanities*, 7(6), 2481-2495.

Nwodo, F. A., & Amucheazi, C. O. (2025). Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's Data Protection Commission. *International Data Privacy Law*, 15(1), 91-100. https://doi.org/10.1093/idpl/ipae021

Obi, U. V. (2020). Data Privacy and Protection Regulations in Nigeria: Challenges Confronting Implementation. International Network of Privacy Law Professionals.

Omotayo, B. (2025, May 14). Talent Shortage Threatens Nigeria's Cybersecurity Resilience. *BusinessDay Nigeria*. https://businessday.ng/companies/article/talent-shortage-threatens-nigerias-cybersecurity-resilience/

Oweh, I. (2025, October 9). Group Laments Limitations to Digital Rights in Nigeria. *Independent Newspaper Nigeria*. https://independent.ng/group-laments-limitations-to-digital-rights-in-nigeria/

Pan-African Parliament. (2026, January 27). *Pan-African Parliament President calls for African Sovereignty over Sensitive Data and AI at Nairobi Conference*. African Union. https://pap.au.int/en/news/press-releases/2026-01-27/pan-african-parliament-president-calls-african-sovereignty-over

Punch Newspapers. (2025, August 29). Cybersecurity Vulnerabilities Threaten Nigeria's Business Landscape – Glemad CEO. https://punchng.com/cybersecurity-vulnerabilities-threaten-nigerias-business-landscape-glemad-ceo/

Ramezan, C. A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. *Journal of Information Systems Education*, *34*(1), 94-105. https://jise.org/volume34/n1/JISE2023v34n1pp94-105.html

Salami, A. O. (2024). Artificial Intelligence, Digital Colonialism, and the Implications for Africa's Future Development. *Data & Policy*, 6, e83. https://doi.org/10.1017/dap.2024.67

Salami, M. (2025, June 6). *Expert Urges Data Domestication to Curb Cyber Threats*. *The Guardian Nigeria* https://guardian.ng/technology/tech/expert-urges-data-domestication-to-curb-cyber-threats/

Sun, S. C., Shabaya, M. M., & Kalema, N. L. (2025). Fostering African Data Commons: Embracing the Philosophy of Ubuntu. In P. Hacker (Ed.), *Oxford Intersections: AI in Society*. Oxford University Press.

The Guardian Nigeria. (2025, October 14). *LASG Promises Sustained Digital Protection at 2025 Cybersecurity Awareness Campaign*. *The Guardia* https://guardian.ng/news/lasg-promises-sustained-digital-protection-at-2025-cybersecurity-awareness-campaign/

The Sun. (2025, October 30). AI Policy without Infrastructure Risk Digital Dependence, Expert Warns. *The Sun*. https://thesun.ng/ai-policy-without-infrastructure-risks-digital-dependence-expert-warns/

Tribune Online. (2024, September 11). FG Trains 518 Youths on Cybersecurity. *Tribune Online*. https://tribuneonlineng.com/fg-trains-518-youths-on-cybersecurity/

Tribune Online. (2025, December 9). Nigeria Lacks AI-Ready Data Centres, Trails in Capacity — Nnamani. *Tribune Online*. https://tribuneonlineng.com/nigeria-lacks-ai-ready-data-centres-trails-in-capacity-nnamani/

Umeh, J. (2025, October 22). Only 23% of Rural Communities Have Internet Access in Nigeria — NCC. *Vanguard News*. https://www.vanguardngr.com/2025/10/only-23-of-rural-communities-have-internet-access-in-nigeria-ncc/