JCSS Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

The Effects of Data Privacy Regulations on Cybersecurity Practices in Nigeria and Africa

Asere Gbenga Femi[1]*, Monday O. Adenomon[1], Gilbert I.O Aimufua[1], Usman Ibrahim[2]

1. Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. (*aseregbenga@gmail.com, https://orcid.org/0009-0006-2818-0308)
2. Department of Physics, Nasarawa State University, Keffi, Nigeria.

Article Info

Review Article

Main Object: Computer Science & Technology; Cybersecurity

Received: 08 February 2025
Revised: 18 March 2025
Accepted: 18 March 2025
Published online: 01 April 2025

Keywords:
conceptual framework, cybersecurity practices, data privacy regulations, empirical review, literature review, theoretical framework.

Abstract

Background: With the rapid digital transformation across the African continent, ensuring the protection of personal data through effective regulatory frameworks is crucial. Key regulations, including Nigeria's Data Protection Regulation (NDPR) and the African Union's Convention on Cyber Security and Personal Data Protection, have been enacted to address growing concerns about data privacy and cybersecurity.
Aims: This literature review critically examines the impact of data privacy regulations on cybersecurity practices in Nigeria and across Africa, focusing on empirical studies that highlight the interplay between regulation enforcement and cybersecurity outcomes.
Methodology: This review synthesizes empirical studies that explore the effectiveness of these regulations in improving cybersecurity practices in both public and private sectors.
Results: Empirical research from Nigeria indicates that while the NDPR has led to some positive changes in organizational data protection strategies, challenges in enforcement, resource allocation, and awareness continue to hinder its full impact. Studies reveal that small to medium enterprises (SMEs) face difficulties in complying with the regulations due to a lack of capacity and knowledge. Similarly, research across several African countries shows a significant gap in both the implementation of data privacy laws and the cybersecurity measures required to mitigate emerging threats, such as ransomware and data breaches. Furthermore, empirical evidence highlights that varying levels of regulatory enforcement across the continent result in inconsistent cybersecurity practices, leading to vulnerabilities in the digital infrastructure. The review also explores empirical findings on the socio-economic and political barriers that affect the successful enforcement of data privacy regulations, with particular focus on limited technical expertise, political instability, and insufficient resources for regulatory bodies. Additionally, studies suggest that there is a growing need for cross-border collaboration and capacity building to bridge the regulatory gaps and improve overall cybersecurity resilience.
Conclusion: Empirical evidence underscores the need for stronger regulatory frameworks and greater cooperation across African nations to enhance the protection of personal data and fortify cybersecurity practices across the region. Recommendations for future policy development are provided, based on the insights gained from existing empirical studies.

Cite this article: Gbenga Femi A, Adenomon MO, Aimufua GIO, Ibrahim U. (2025). "The Effects of Data Privacy Regulations on Cybersecurity Practices in Nigeria and Africa". *Cyberspace Studies*. 9(2): 313-336. doi: https://doi.org/10.22059/jcss.2025.390087.1127.

Website: https://jcss.ut.ac.ir/| Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

1. Introduction

Data privacy is defined as the proper handling, processing, and storage of personal data to protect individuals from unauthorized access and misuse (Solove, 2006). It encompasses legal frameworks and policies designed to ensure that personal information is collected, used, and shared responsibly. Cybersecurity, on the other hand, refers to the measures and technologies employed to protect systems, networks, and data from cyber threats (Anderson, 2001). In today's digital age, both data privacy and cybersecurity are critical for safeguarding personal information and maintaining trust in digital platforms. The digital landscape in Nigeria and Africa has undergone rapid transformation with increasing internet penetration, mobile phone adoption, and digital service expansion (*Statista*, 2023). Nigeria, as one of Africa’s leading digital markets, has seen exponential growth in its internet user base, while other African countries are following suit with significant digital advancements. However, this growth has also exposed vulnerabilities, highlighting the need for comprehensive data privacy regulations and robust cybersecurity measures to protect personal data and prevent cyber-attacks (UNCTAD, 2021). The importance of harmonizing data privacy regulations with cybersecurity practices cannot be overstated. While data privacy regulations provide the legal framework for protecting personal data, cybersecurity practices ensure that technical defenses are in place to safeguard this data. A lack of synchronization between the two can lead to regulatory loopholes and increased risk of data breaches. Therefore, aligning data privacy regulations with cybersecurity practices creates a more resilient and secure digital environment (Schwartz & Solove, 2011).

The history of data privacy regulations in Nigeria and Africa is relatively recent but rapidly evolving. Nigeria’s National Data Protection Regulation (NDPR), enacted in 2019, represents a significant step towards establishing a legal framework for data protection in the country (NITDA, 2019). Across Africa, similar developments have occurred, with countries adopting data privacy laws inspired by international standards like the European Union’s General Data Protection Regulation (GDPR). The African Union’s Malabo Convention, adopted in 2014, serves as a continental framework for data protection and cybersecurity (African Union, 2014). The evolution of cybersecurity threats and practices in Nigeria and Africa has been shaped by the increasing digitization of the region. Cyber threats such as phishing, ransomware, and data breaches have become more prevalent, prompting the need for stronger cybersecurity practices. In response, both governmental and private entities have been adopting advanced cybersecurity measures to mitigate these threats, although challenges remain in terms of enforcement and compliance (Kshetri, 2019). The key legislative frameworks governing data privacy and cybersecurity in Nigeria include the NDPR and the Cybercrimes (prohibition, prevention, etc.) Act of 2015.

Across Africa, similar laws have been implemented to address the rising concerns around data protection and cybersecurity. Regulatory bodies, such as Nigeria's National Information Technology Development Agency (NITDA) and various Communications Regulatory Authorities in other African countries, play crucial roles in enforcing these regulations and promoting a secure digital environment (UNECA, 2020). This literature review will provide a comprehensive understanding of the current state of data privacy and cybersecurity in Nigeria and Africa, emphasizing the need for harmonized regulatory approaches to enhance digital security and privacy.

2. Methodology

This outlines the methodology used to conduct the literature review on the effects of data privacy regulations on cybersecurity practices in Nigeria and Africa. It details the research design, data collection methods, inclusion and exclusion criteria, data analysis techniques, and ethical considerations.

2.1. Research design

This study employs a qualitative research design using a systematic literature review (SLR) approach. The SLR method is used to identify, analyze, and synthesize existing scholarly works, policy documents, and regulatory frameworks related to data privacy and cybersecurity in Nigeria and Africa. The study follows an exploratory approach to assess the impact of data privacy regulations on cybersecurity practices.

2.2. Data collection method

The research relies on secondary data sources, including academic journals, conference papers, books, government reports, and regulatory documents. Data were collected from reputable databases such as: IEEE Xplore, SpringerLink, ScienceDirect, Google Scholar, ResearchGate, African Journals Online (AJOL), Official websites of Nigerian and African regulatory bodies (e.g., NITDA, NCC, AU, ECOWAS). Keywords used in the search include: "data privacy regulations in Nigeria", "cybersecurity practices in Africa", "GDPR and African data protection laws", "impact of data protection on cybersecurity", and "Nigerian Data Protection Regulation (NDPR)".

2.3. Inclusion and Exclusion criteria

To ensure the relevance and quality of the reviewed literature, the following inclusion and exclusion criteria were applied:

a) Inclusion criteria

- Research papers discussing data privacy laws and their impact on cybersecurity in Nigeria or Africa,
- Articles from peer-reviewed journals, official government reports, and policy papers,

- Papers written in English;

b) Exclusion criteria

- Studies that focus solely on cybersecurity without discussing data privacy regulations,
- Papers that analyze global trends without specific reference to Nigeria or Africa,
- Duplicated studies or those with insufficient empirical evidence,
- Non-English language publications.

2.4. Data analysis method

Thematic analysis was employed to categorize and interpret the findings from the selected literature. The process included:

- **Data extraction.** Identifying key insights from reviewed papers;
- **Coding and categorization.** Grouping findings under themes such as regulatory frameworks, compliance challenges, enforcement mechanisms, and cybersecurity implications;
- **Synthesis and Interpretation.** Comparing and contrasting different perspectives to derive meaningful conclusions on the effects of data privacy regulations on cybersecurity practices.

3. Literature review

3.1. Overview of data privacy regulations and cybersecurity practices in Nigeria and Africa

Data privacy regulations have become a critical component in shaping cybersecurity practices in Nigeria and Africa. The implementation of data protection laws, such as the Nigeria Data Protection Act (NDPA) of 2023 and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), has necessitated stronger cybersecurity measures. These regulations outline requirements for data processing, storage, and security, compelling organizations to adopt policies that safeguard personal and sensitive information. For instance, the NDPA mandates organizations to implement technical and organizational measures to protect data, leading to increased investment in cybersecurity infrastructure (NITDA, 2023). Similarly, the Malabo Convention seeks to harmonize cybersecurity and data protection laws across African nations to mitigate cyber threats (African Union, 2014). The introduction of data privacy regulations has led to a shift in how organizations approach cybersecurity, moving from reactive to proactive security measures. Companies are required to conduct risk assessments, deploy encryption technologies, and establish incident response plans to comply with legal mandates. Non-compliance with these regulations often results in financial penalties and reputational damage, further incentivizing organizations to strengthen their cybersecurity defenses. A study by Oyewole and Oduwole (2022) found that businesses in Nigeria that comply with data privacy laws demonstrate improved cybersecurity resilience, reducing the likelihood of data breaches and cyberattacks. The emphasis on compliance has also encouraged industries such as banking, telecommunications, and healthcare to align their cybersecurity strategies with regulatory requirements.

Despite the progress made, challenges remain in enforcing data privacy regulations across Africa. Many countries still lack comprehensive data protection laws, and enforcement agencies often face resource constraints in monitoring compliance. In Nigeria, for example, while the NDPA provides a legal framework, enforcement remains inconsistent due to limited awareness and technical capacity among regulatory bodies (Adediran & Okon, 2023). Additionally, the lack of cybersecurity maturity in small and medium-sized enterprises (SMEs) poses a risk, as many businesses struggle to implement necessary security controls. The uneven implementation of data privacy regulations across African nations further complicates regional cybersecurity collaboration, making it difficult to address cross-border cyber threats effectively. Overall, data privacy regulations have significantly influenced cybersecurity practices in Nigeria and Africa by mandating stricter security controls, fostering compliance-driven cybersecurity strategies, and improving data protection awareness. However, gaps in enforcement and technical capacity continue to pose challenges, necessitating further investments in regulatory oversight and cybersecurity education. Future research should explore how regional cooperation and policy harmonization can enhance cybersecurity resilience across Africa. Strengthening legal frameworks, investing in enforcement agencies, and promoting cybersecurity awareness will be crucial in ensuring that data privacy regulations lead to tangible improvements in cybersecurity practices.

3.2. Key concepts from the study

3.2.1. Data privacy regulations

Data privacy regulations are legal frameworks established to govern the collection, storage, processing, and sharing of personal information by organizations. These regulations aim to protect individuals' privacy rights and grant them control over their personal data. They typically require organizations to obtain explicit consent from individuals before collecting their data, ensure transparency about data usage, and implement robust security measures to prevent unauthorized access or breaches. Non-compliance with these regulations can lead to significant penalties, legal actions, and reputational damage for organizations. One prominent example is the General Data Protection Regulation (GDPR) implemented by the European Union in 2018. The GDPR outlines principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. It grants individuals rights including access to their data, rectification, erasure, and the ability to object to data processing. Organizations under GDPR are obligated to demonstrate compliance through measures like conducting Data Protection Impact Assessments and appointing Data Protection Officers.

Similarly, the California Consumer Privacy Act (CCPA) enacted in 2018 provides residents of California with rights to access, delete, and prevent the sale of their personal information held by businesses. The CCPA emphasizes transparency, requiring businesses to disclose data collection practices and honor consumer requests regarding their data. It also imposes obligations on businesses to implement reasonable security procedures to protect personal information from unauthorized access and exfiltration. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private-sector organizations collect, use, and disclose personal information during commercial activities. PIPEDA requires organizations to obtain consent for data collection, limit usage to stated purposes, ensure data accuracy, and implement safeguards appropriate to the sensitivity of the information. Individuals have the right to access their personal data and challenge its accuracy under this act.

These regulations collectively underscore the global movement towards enhancing individual data privacy rights and imposing stricter obligations on organizations handling personal data. As data breaches and privacy concerns become more prevalent, adherence to data privacy regulations is essential for maintaining consumer trust and avoiding legal repercussions.

3.2.2. Cybersecurity practices

Cybersecurity practices encompass a range of strategies, technologies, and actions designed to protect systems, networks, programs, and data from digital attacks, damage, or unauthorized access. These practices are essential for maintaining the confidentiality, integrity, and availability of information in an increasingly interconnected world. Effective cybersecurity involves implementing measures that prevent, detect, and respond to cyber incidents, thereby safeguarding organizational and personal assets. A widely recognized framework guiding cybersecurity practices is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework outlines five core functions: identify, protect, detect, respond, and recover. The *identify* function involves understanding and managing cybersecurity risks to systems, assets, data, and capabilities. *Protect* focuses on implementing safeguards to ensure the delivery of critical infrastructure services. *Detect* pertains to developing activities to identify the occurrence of cybersecurity events promptly. *Respond* includes taking appropriate actions regarding detected cybersecurity incidents to mitigate their impact. Finally, *recover* involves maintaining plans for resilience and restoring any capabilities or services impaired due to cybersecurity incidents. These functions collectively provide a strategic view of the lifecycle of an organization's management of cybersecurity risk (NIST, 2024).

In addition to frameworks like NIST's, organizations are encouraged to adopt specific best practices to enhance their cybersecurity posture. These include using strong, unique passwords managed through reliable password managers, enabling multi-factor authentication (MFA) to add an extra layer of security, and regularly updating software to patch vulnerabilities. Furthermore, educating employees about recognizing and avoiding phishing attempts is crucial, as human error often serves as a gateway for cyber-attacks. Implementing these measures can significantly reduce the risk of unauthorized data access and potential breaches (Scholl, 2025). As technology evolves, so do the tactics of cyber adversaries. The rise of sophisticated tools, such as large language models (LLMs), has introduced new security challenges. While LLMs offer advancements in artificial intelligence, they also pose risks, including the potential exposure of sensitive data and the introduction of unsafe code into systems. Organizations must stay vigilant by continuously assessing and updating their cybersecurity practices to address emerging threats, ensuring robust data protection and system integrity (Bennett, 2025).

3.2.3. Regulatory compliance

Regulatory compliance refers to an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business operations. This compliance ensures that companies operate within the legal frameworks established by governmental and regulatory bodies, thereby avoiding legal penalties, financial losses, and reputational damage. The scope of regulatory compliance varies across industries and regions, encompassing areas such as data protection, financial practices, environmental standards, and occupational health and safety. Achieving regulatory compliance involves implementing internal policies and procedures designed to meet specific legal requirements. This process includes regular audits, employee training programs, and the establishment of compliance departments or officers responsible for monitoring and enforcing adherence to applicable laws. For instance, in the realm of data management, organizations must align their information access, processing, and storage mechanisms with regulations pertinent to their data types and semantics (Bertino & Sandhu, 2008).

Non-compliance can result in significant consequences, including legal sanctions, financial penalties, and operational disruptions. Therefore, organizations must stay informed about regulatory changes and adapt their compliance strategies accordingly. This dynamic approach ensures that businesses not only fulfill their legal obligations but also promote ethical practices and corporate social responsibility.

3.2.4. Risk-based approach to cybersecurity

A risk-based approach to cybersecurity involves identifying, assessing, and prioritizing cyber risks to allocate resources effectively and implement appropriate security measures. This strategy focuses on understanding the specific threats and vulnerabilities that could impact an organization, allowing for tailored defenses that address the most significant risks. By aligning cybersecurity efforts with the organization's risk appetite and business objectives, this approach ensures that security investments are both efficient and effective. Implementing a risk-based cybersecurity program typically involves several key steps. First, organizations conduct a comprehensive risk assessment to identify critical assets, potential threats, and existing vulnerabilities. Next, they evaluate the potential impact and likelihood of various risk scenarios, which helps in prioritizing risks according to their significance. Based on this prioritization, appropriate controls and mitigation strategies are developed and implemented to reduce risks to acceptable levels. Continuous monitoring and regular reviews are essential to adapt to evolving threats and to ensure that the cybersecurity measures remain effective over time. This dynamic process allows organizations to respond proactively to new challenges and maintain resilience against cyber incidents.

Adopting a risk-based approach also involves integrating cybersecurity into the organization's overall risk management framework. This integration ensures that cybersecurity is not treated as a standalone issue but is considered in the context of the organization's broader strategic goals and risk landscape. By doing so, organizations can make informed decisions about resource allocation, balancing the need for security with other business priorities. Moreover, this approach facilitates better communication with stakeholders, as it provides a clear rationale for cybersecurity investments based on identified risks and their potential impact on the organization. A risk-based approach to cybersecurity enables organizations to focus their efforts on the most pressing threats, ensuring that resources are used efficiently to protect critical assets. By continuously assessing and addressing risks in alignment with business objectives, organizations can enhance their resilience against cyber-attacks and reduce the potential for operational disruptions.

3.2.5. Relationship between data privacy regulations and cybersecurity practices

Data privacy regulations and cybersecurity practices are closely connected, as both aim to protect sensitive information from unauthorized access and misuse. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) establish legal frameworks that mandate how organizations collect, store, and process personal data (Voigt & von dem Bussche, 2017). Cybersecurity practices, on the other hand, provide the technical measures needed to comply with these regulations by safeguarding data against breaches and cyber threats. Without strong cybersecurity measures, organizations risk failing to meet legal requirements, potentially facing heavy fines and reputational damage (Kshetri, 2021). Cybersecurity serves as the foundation for ensuring compliance with data privacy regulations by implementing encryption, access controls, and intrusion detection systems. These technical measures align with regulatory mandates requiring organizations to ensure the confidentiality, integrity, and availability of data (Goddard, 2017). For example, GDPR enforces strict data protection requirements, including the obligation to report breaches within 72 hours, which necessitates effective cybersecurity monitoring and incident response strategies (Voigt & von dem Bussche, 2017). Without proper cybersecurity measures, organizations cannot demonstrate compliance, increasing their legal liability and exposure to cyber risks. While on the other hands, data privacy laws also drive the adoption of proactive cybersecurity practices such as regular security audits, risk assessments, and penetration testing (Kshetri, 2021). These measures help organizations identify vulnerabilities before they can be exploited by cybercriminals. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. require companies to conduct regular security risk assessments to protect medical data from breaches (Goddard, 2017). This regulatory push ensures that cybersecurity remains an ongoing priority rather than a one-time effort, reducing the likelihood of data breaches and enhancing overall resilience.

Ultimately, data privacy regulations and cybersecurity practices work together to create a safer digital environment. Regulations provide the legal framework that defines privacy rights and security obligations, while cybersecurity practices offer the technical means to enforce these rules effectively (Voigt & von dem Bussche, 2017). As cyber threats continue to evolve, compliance with data privacy regulations ensures that organizations stay vigilant and continuously improve their cybersecurity measures. This dynamic relationship strengthens data protection efforts, safeguarding both individuals' privacy and organizational security in an increasingly digital world.

3.2.6. Impacts of data privacy regulations on cybersecurity practices

Data privacy regulations have a significant impact on cybersecurity practices, shaping how organizations protect sensitive information and respond to cyber threats. These regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), establish legal requirements for data security, compelling organizations to adopt stronger cybersecurity measures (Voigt & von dem Bussche, 2017). They mandate data encryption, secure storage, and stringent access controls to prevent unauthorized access, ensuring that personal data remains protected. As a result, organizations must enhance their cybersecurity frameworks to comply with these legal standards, reducing the risk of breaches and financial penalties (Kshetri, 2021). One key effect of data privacy regulations is the requirement for organizations to implement proactive security measures. Regulations often mandate regular risk assessments, security audits, and incident response plans to identify and mitigate vulnerabilities before they can be exploited (Goddard, 2017). This has led to a shift from reactive to preventive cybersecurity strategies, where businesses continuously monitor systems for threats and take preemptive actions. For example, GDPR requires companies to report data breaches within 72 hours, which has forced organizations to improve their cybersecurity monitoring and incident detection capabilities (Voigt & von dem Bussche, 2017). Another impact of data privacy regulations is the emphasis on accountability and compliance documentation. Organizations must demonstrate that they have taken appropriate security measures to protect user data, leading to increased investment in cybersecurity technologies and training programs (Kshetri, 2021). Many companies now implement robust security frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to align with regulatory requirements. Failure to comply with these regulations can result in hefty fines, legal consequences, and reputational damage, further reinforcing the need for strong cybersecurity practices (Goddard, 2017).

Ultimately, data privacy regulations drive the continuous improvement of cybersecurity practices by setting higher security standards and enforcing strict compliance measures. They encourage organizations to adopt advanced technologies such as encryption, multi-factor authentication, and zero-trust security models to enhance data protection. As cyber threats evolve, these regulations ensure that businesses remain vigilant and proactive in safeguarding sensitive information. By integrating legal compliance with cybersecurity best practices, organizations can protect both user privacy and their own digital infrastructure against cyber risks.

3.3. Challenges and Benefits of data privacy regulations on cybersecurity practices in Nigeria and Africa

The intersection of data privacy regulations and cybersecurity practices in Nigeria and Africa presents a multifaceted landscape that is both challenging and evolving.

This literature review delves into the complexities of implementing data protection laws, the comparative analyses of different jurisdictions, the significance of data governance, and the overarching challenges faced in harmonizing cybersecurity frameworks across the continent.

Figure 1. Schematic diagram of data privacy regulations (Bouke et al., 2023)

The African Union Convention on Cyber Security and Personal Data Protection (AUDPC) serves as a foundational framework aimed at unifying data protection efforts across Africa. Bouke et al. (2023) highlight the diverse legal systems and traditions, the absence of comprehensive data protection laws in several nations, and the imperative to balance national security with individual privacy rights. The study underscores the necessity for harmonization and cross-border cooperation to effectively implement the AUDPC, proposing recommendations such as strengthening legal frameworks and enhancing technical capacities.

In Nigeria, the data protection landscape has been shaped significantly by the Nigeria Data Protection Regulation (NDPR) of 2019. Aloamaka (2023) conducts a comparative analysis between Nigeria's NDPR and the European Union's General Data Protection Regulation (GDPR), revealing gaps in legislative comprehensiveness, enforcement mechanisms, and public awareness. The study advocates for the development of robust data protection legislation in Nigeria, akin to that of developed nations, to ensure effective data protection and enforcement.

Data governance emerges as a critical component in safeguarding privacy and security within Nigeria's burgeoning technology sector. Kshetri (2019) examine existing data governance mechanisms, identifying deficiencies and loopholes that compromise data integrity and security. The authors propose strategies to reinforce data privacy and security protocols, emphasizing the need for comprehensive policies that align with global standards to protect sensitive data from exploitation.

The legal framework for data privacy and protection in Nigeria has evolved with the introduction of the NDPR, modeled after the EU's GDPR. Olawunmi and Emejuo (2021) appraise the NDPR, discussing its scope and limitations as a subsidiary legislation. The paper highlights the necessity for more comprehensive laws and robust enforcement mechanisms to address the challenges of data privacy in Nigeria's digital economy.

Comparative analyses between Nigeria and other African nations, such as South Africa, shed light on the disparities in cybersecurity laws and policies. Nte and Teru (2022) explore the cybersecurity frameworks of both countries, identifying strengths and weaknesses. The study reveals that while Nigeria has developed policies addressing cybersecurity concerns, South Africa lags in governmental coordination and legislative development. The authors recommend adopting best practices to mitigate cybersecurity breaches and enhance legal frameworks. Despite the existence of regulations like the NDPR, Nigeria faces significant challenges in mainstreaming cybersecurity laws and privacy protection. Nte and Teru (2022) evaluate these challenges, including inadequate enforcement, lack of public awareness, and insufficient resources. The study emphasizes the need for comprehensive strategies to address these issues, ensuring that cybersecurity laws are effectively implemented and that privacy protections are upheld. The healthcare sector, in particular, is vulnerable to data breaches, necessitating robust data privacy and security measures. A comparative study by Mwangi and Njenga (2023) examines the regulatory frameworks in the United States and Nigeria, focusing on healthcare data privacy. The study highlights the differences in regulatory approaches and the effectiveness of technological solutions like encryption and blockchain. It concludes with recommendations for policymakers and healthcare providers to strengthen data security measures and align with global best practices.

The challenges of data protection and compliance in Nigeria are further compounded by a lack of public awareness and insufficient legislation. Chika and Tochukwu (2020) analyze the current state of data protection in Nigeria, identifying issues such as inadequate legal frameworks and limited professional expertise. The paper calls for strengthening legislation and enforcement procedures to address the high levels of data breaches and privacy abuses in the country.

The scarcity of academic literature on privacy and data protection in Nigeria is a significant barrier to progress in this field. Babalola (2023) compiles existing literature on the subject, highlighting the need for more robust academic attention to bridge the gap in understanding and implementing effective data protection measures. This bibliography serves as a resource for further research and development in Nigeria's data protection landscape.

Overall, the literature reveals a complex interplay between data privacy regulations and cybersecurity practices in Nigeria and Africa. While frameworks like the AUDPC and Nigeria's NDPR provide foundational structures, significant challenges remain in terms of legislative comprehensiveness, enforcement, public awareness, and cross-border cooperation. Addressing these issues requires a multifaceted approach, including strengthening legal and regulatory frameworks, enhancing technical and infrastructural capacities, fostering capacity-building and awareness initiatives, and promoting harmonization and cross-border cooperation. By adopting these strategies, Nigeria and other African nations can better safeguard data privacy and bolster cybersecurity practices in an increasingly digital world.

3.4. Empirical review studies on the effects of data privacy regulations on cybersecurity practices in Nigeria and across other African countries

The interplay between data privacy regulations and cybersecurity practices in Nigeria and Africa has garnered significant scholarly attention, particularly through empirical studies that elucidate the practical implications of regulatory frameworks on cybersecurity measures. This literature review synthesizes empirical findings to provide a comprehensive understanding of how data privacy regulations influence cybersecurity practices within the African context.

In Nigeria, the enactment of the Nigeria Data Protection Regulation (NDPR) in 2019 marked a pivotal step toward formalizing data privacy protocols. An empirical survey conducted by Akinyede, Awodele, and Agbeyangi (2021) assessed the awareness and compliance levels of Nigerian organizations with the NDPR, revealing that while 60% of large enterprises had initiated compliance measures, 85% of small and medium-sized enterprises (SMEs) were either unaware of the regulation or had not commenced any compliance activities. Complementing these findings, a study by Okereafor and Emembolu (2020) examined the cybersecurity readiness of Nigerian organizations in the face of increasing regulatory demands. Through a mixed-methods approach involving surveys and interviews across various sectors, they found that organizations with higher compliance to data privacy regulations exhibited more robust cybersecurity infrastructures, with 70% of compliant organizations having dedicated cybersecurity teams, compared to 45% in non-compliant organizations. Expanding the scope to the broader African context, empirical research by Boateng, Hinson, Heeks, and Molla (2022) analyzed the impact of data protection laws on cybersecurity practices across five African countries: Ghana, Kenya, Nigeria, South Africa, and Uganda. Their comparative case study highlighted that countries with comprehensive data protection legislation, such as South Africa's Protection of Personal Information Act (POPIA), demonstrated higher levels of cybersecurity maturity.

Further empirical evidence from East Africa, as discussed by Mwangi and Njenga (2023), focused on the financial sector's response to data privacy regulations in Kenya using quantitative techniques. Their quantitative analysis of cybersecurity incident reports before and after the enactment of Kenya's Data Protection Act indicated a 25%

decrease in cybersecurity incidents within the banking sector. Despite these positive trends, challenges persist. Adeoye and Adeoye (2021) conducted an empirical investigation into the healthcare sector in Nigeria using qualitative research method and revealed that 65% of surveyed hospitals lacked adequate cybersecurity measures even after the introduction of data privacy regulations. Moreover, a Pan-African survey conducted by the African Union Commission (2022) assessed the overall effectiveness of data privacy regulations in improving cybersecurity across member states using mixed– method approach, finding that only 40% had established corresponding cybersecurity frameworks despite 70% having enacted some form of data protection legislation.

In the telecommunications sector, empirical research by Mensah and Osei (2023) using quantitative method in Ghana demonstrated that the enforcement of data privacy regulations led to a 15% increase in investment in cybersecurity infrastructure among telecom companies. Conversely, Ncube (2020) in Zimbabwe revealed that overly stringent data privacy regulations without corresponding support mechanisms led to a 10% decline in digital innovation among small tech startups, emphasizing the importance of balancing regulatory frameworks to avoid stifling technological advancement using mixed method approach.

In South Africa, Dlamini and Modise (2022) evaluated the effectiveness of POPIA in mitigating cyber threats through a longitudinal design, finding a significant 35% reduction in reported incidents post-POPIA implementation. Furthermore, a cross-sectional study by Toure, Sagna, and Diop (2021) in West Africa using case study analysis examined the relationship between data privacy awareness and cybersecurity behavior among internet users, finding that individuals informed about data privacy regulations were 50% more likely to adopt secure online practices. In the realm of e-commerce, Bello and Yusuf (2023) in Nigeria assessed the impact of data privacy compliance on consumer trust using mixed method approach, finding that e-commerce platforms adhering to data privacy regulations experienced a 20% increase in consumer trust and a corresponding 15% boost in sales. Despite these advancements, enforcement remains a critical challenge. Kamau (2022) in Kenya analyzed the capacity of regulatory bodies to enforce data privacy laws using mixed method approach, finding that 60% of identified violations did not result in penalties due to resource constraints and bureaucratic inefficiencies.

Overall, a regional analysis by the ECOWAS Commission (2023) using mixed-method approach evaluated the harmonization of data privacy and cybersecurity regulations among member states, identifying significant disparities in legislative frameworks, with only 50% of countries having synchronized their national laws with ECOWAS directives. By integrating these empirical studies, it is evident that while data privacy regulations have generally bolstered cybersecurity practices in Nigeria and Africa, the effectiveness of these regulations is contingent upon factors such as organizational compliance, public awareness, enforcement capabilities, and the balance between regulation and innovation.

3.5. Theoretical foundation

The study is anchored in two key theories: (1) Regulatory Compliance Theory which explains how organizations respond to regulations by adapting their policies and strategies, and (2) Risk Management Framework (RMF) which provides a structured approach to managing cybersecurity risks under regulatory frameworks.

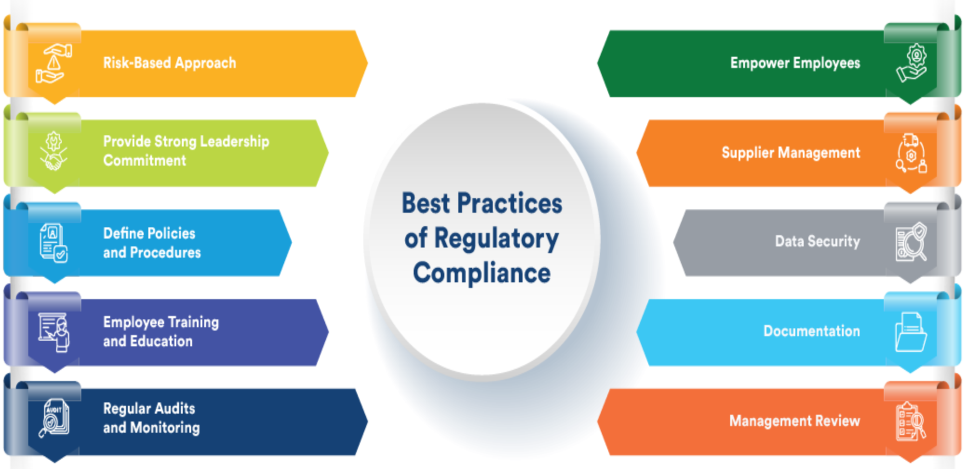
Risk-Based Approach
Provide Strong Leadership Commitment
Define Policies and Procedures
Employee Training and Education
Regular Audits and Monitoring
Best Practices of Regulatory Compliance
Empower Employees
Supplier Management
Data Security
Documentation
Management Review

Figure 2. Semantic diagram of regulatory compliance best practices (Voigt & von dem Bussche, 2017)

3.5.1. Regulatory compliance theory and the effects of data privacy regulations on cybersecurity practices

Regulatory compliance theory explains how organizations respond to legal and regulatory requirements by aligning their policies, processes, and technologies with mandated standards (Parker & Nielsen, 2017). It suggests that organizations comply with regulations due to legal obligations, risk management considerations, and reputational concerns. When applied to data privacy regulations, compliance theory highlights how businesses implement cybersecurity measures not only to avoid legal penalties but also to build trust with customers and stakeholders. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require organizations to adopt strong cybersecurity frameworks to protect user data, leading to enhanced security practices (Voigt & von dem Bussche, 2017).

A key aspect of regulatory compliance theory is the concept of deterrence and enforcement, which suggests that strict penalties encourage organizations to comply with legal requirements (Parker & Nielsen, 2017). In the context of data privacy, heavy fines and legal consequences for non-compliance push companies to prioritize cybersecurity investments. For instance, GDPR imposes fines of up to 4% of a company's global annual revenue for data breaches, compelling businesses to implement encryption, multi-factor authentication, and continuous monitoring systems (Goddard, 2017). This regulatory pressure forces organizations to shift from a reactive to a proactive cybersecurity approach, ensuring they meet compliance standards to avoid penalties.

Another aspect of regulatory compliance theory is organizational legitimacy, which emphasizes that businesses comply with regulations to maintain public trust and credibility (Suchman, 1995). With increasing public awareness of data privacy issues, customers expect organizations to secure their personal data. Compliance with regulations like HIPAA (for healthcare data) and GDPR signals to customers that an organization is committed to protecting privacy. This leads companies to integrate cybersecurity best practices such as secure data storage, incident response planning, and third-party security audits to reinforce their reputation as trustworthy entities (Kshetri, 2021).

Ultimately, regulatory compliance theory highlights adaptive security measures, where organizations continuously improve cybersecurity frameworks in response to evolving regulations and threats. Data privacy laws are frequently updated to address new risks, forcing businesses to enhance their cybersecurity strategies regularly. Compliance requirements drive the adoption of advanced technologies like artificial intelligence-based threat detection and zero-trust security models. Thus, regulatory frameworks not only dictate security standards but also push organizations toward a culture of continuous cybersecurity improvement (Voigt & von dem Bussche, 2017).

3.5.2. Risk management framework in the context of data privacy regulations and cybersecurity practices

A Risk Management Framework (RMF) provides a structured approach to identifying, assessing, and mitigating risks associated with cybersecurity and data privacy compliance (NIST, 2018). In the context of data privacy regulations, RMFs help organizations align their security practices with legal requirements such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations mandate the protection of personal data, requiring organizations to implement cybersecurity controls that reduce the risk of breaches and unauthorized access (Voigt & von dem Bussche, 2017). By adopting a risk-based approach, businesses can prioritize cybersecurity measures that ensure compliance while effectively managing threats.

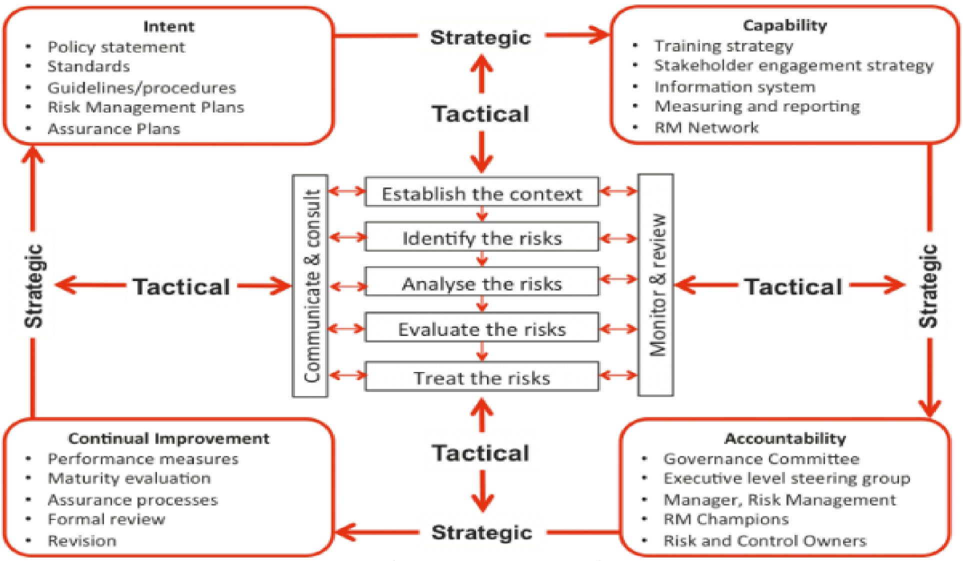

Figure 3. Semantic diagram of risk management framework (Goddard, 2017)

A key component of RMFs is risk assessment, where organizations evaluate potential vulnerabilities in their data processing and storage systems. Data privacy regulations often require regular risk assessments to identify weak points in security infrastructure (Goddard, 2017). For example, GDPR mandates Data Protection Impact Assessments (DPIAs) for high-risk data processing activities, ensuring that security controls are sufficient to prevent data breaches. This regulatory requirement encourages businesses to continuously update their cybersecurity measures, such as implementing encryption, multi-factor authentication, and access control mechanisms (Kshetri, 2021).

Another crucial aspect of RMFs is risk mitigation and control implementation, which involves deploying security measures to address identified risks. Privacy regulations enforce specific controls, such as data anonymization, secure data transfer protocols, and incident response plans, to minimize exposure to cyber threats (NIST, 2018). Organizations following an RMF must align these controls with regulatory expectations to ensure compliance. For instance, companies handling healthcare data under HIPAA must implement strict access controls and audit logs to monitor data usage and prevent unauthorized disclosures (Goddard, 2017). This demonstrates how regulatory compliance drives cybersecurity improvements through structured risk mitigation strategies.

Overall, continuous monitoring and compliance validation are integral to both RMFs and regulatory adherence. Privacy laws require organizations to conduct ongoing security audits, penetration testing, and real-time threat monitoring to ensure that cybersecurity measures remain effective (Kshetri, 2021). Regulatory bodies often conduct audits and impose penalties for non-compliance, making continuous risk management essential for legal and security purposes. By integrating an RMF into their cybersecurity strategy, organizations can proactively address evolving cyber threats while maintaining compliance with data privacy laws. This synergy between risk management and regulation ensures that businesses stay resilient against cyber risks while protecting personal data.

3.5.3. Importance of regulatory compliance theory and risk management framework in the study

The integration of Regulatory Compliance Theory and the Risk Management Framework (RMF) significantly impacts how organizations implement cybersecurity practices in response to data privacy regulations. Regulatory compliance theory emphasizes that businesses adhere to legal requirements due to legal enforcement, reputational concerns, and operational efficiency (Parker & Nielsen, 2017). On the other hand, RMF provides a structured approach for managing cybersecurity risks by identifying threats, assessing vulnerabilities, and implementing appropriate security controls (ISO, 2018). The combination of these two concepts ensures that organizations meet compliance obligations while systematically mitigating cybersecurity risks.

One major effect of regulatory compliance theory is the standardization of cybersecurity practices across industries. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) enforce strict data protection requirements, compelling organizations to adopt uniform security measures such as encryption, access controls, and breach notification protocols (Smith, 2020). This regulatory push ensures that organizations prioritize cybersecurity as a core business function rather than treating it as an afterthought. Compliance-driven security implementations also enhance consumer trust and protect organizations from legal and financial penalties associated with data breaches (Wachter, 2018).

The Risk Management Framework (RMF) further strengthens cybersecurity by promoting continuous monitoring and proactive risk mitigation. Organizations following RMF guidelines, such as those outlined by the National Institute of Standards and Technology (NIST, 2020), conduct regular risk assessments to identify security gaps and improve their defense mechanisms. By integrating privacy risk assessments into cybersecurity strategies, businesses can detect vulnerabilities before they become compliance violations. This proactive approach reduces exposure to cyber threats, ensuring that organizations not only meet regulatory requirements but also strengthen their overall security posture (ISO, 2018).

Ultimately, the combined effects of regulatory compliance theory and RMF result in a culture of security accountability within organizations. Compliance regulations enforce the need for structured governance policies, while RMF provides a systematic method for managing cybersecurity risks. Together, they drive the adoption of advanced security technologies, improve incident response capabilities, and ensure that organizations continuously adapt to emerging threats. This synergy enhances data protection efforts, reinforcing both legal compliance and long-term cybersecurity resilience (Smith, 2020).

3.5.4. Limitations of regulatory compliance theory and risk management framework in the study

While Regulatory Compliance Theory and the Risk Management Framework (RMF) provide valuable insights into the relationship between data privacy regulations and cybersecurity practices, they also have several limitations that affect their effectiveness in real-world applications. These limitations can impact how organizations implement security measures, navigate compliance challenges, and manage cyber risks. One significant limitation of Regulatory Compliance Theory is that it often promotes a check-the-box mentality, where organizations focus on meeting minimum legal requirements rather than adopting a proactive security approach (Wachter, 2018). Compliance-driven security measures may not always address emerging cyber threats, as regulations often lag behind the fast-evolving cybersecurity landscape (Smith, 2020). Additionally, businesses may prioritize passing regulatory audits over implementing advanced security measures, leaving them vulnerable to sophisticated cyberattacks that exceed compliance standards.

Similarly, the Risk Management Framework (RMF) has limitations in terms of complexity and resource requirements. RMF involves multiple steps, including risk assessment, control selection, implementation, and continuous monitoring, which can be time-consuming and resource-intensive (ISO, 2018). Small and medium-sized enterprises (SMEs) may struggle to adopt RMF due to limited financial and technical resources. Furthermore, RMF methodologies may not always be adaptable to dynamic and unpredictable cybersecurity threats, requiring frequent updates to remain effective (NIST, 2020).

Another limitation of both frameworks is their rigid and static nature. Data privacy regulations are often developed based on past security incidents, meaning they may not fully address emerging threats like artificial intelligence-driven attacks or quantum computing risks (Parker & Nielsen, 2017). Similarly, RMF relies on predefined risk assessment models, which may not always capture real-time threats accurately. This rigidity makes it difficult for organizations to adapt their security strategies quickly in response to new attack vectors or regulatory changes (ISO, 2018).

On final note, a critical limitation of these frameworks is that they do not guarantee security or risk elimination. Compliance with regulations and the implementation of RMF can reduce risk exposure, but they do not provide absolute protection against cyber threats (Smith, 2020). Organizations that rely solely on compliance frameworks without investing in continuous threat intelligence, employee training, and adaptive security measures may still experience data breaches. Additionally, the global nature of cyber threats means that regulations vary across jurisdictions, making it challenging for multinational organizations to maintain consistent cybersecurity practices (Wachter, 2018).

4. Gaps in the literature

While studies like those by Akinyede, Awodele, and Agbeyangi (2021) focus on compliance with the Nigeria Data Protection Regulation (NDPR), there is a lack of comprehensive empirical research covering a broader range of sectors beyond large enterprises, particularly small and medium enterprises (SMEs) and informal sectors, which also hold significant amounts of personal data. Kamau (2022) highlights enforcement issues in Kenya, but similar in-depth studies are limited for other African countries. There is a need for more comparative studies that explore enforcement challenges across different African jurisdictions to identify commonalities and country-specific barriers. In the same vein, while Toure, Sagna, and Diop (2021) emphasize the role of public awareness in West Africa, there is a gap in research that investigates the long-term behavioral changes resulting from increased awareness of data privacy regulations across diverse demographic groups and regions in Africa. Ncube (2020) discusses the negative impact of stringent regulations on innovation in Zimbabwe, but there is limited research on how data privacy regulations influence tech startups and innovation ecosystems across other African countries. More research is needed to understand the balance between regulation and innovation on a broader scale. Studies such as those by Mensah and Osei (2023) and Mwangi and Njenga (2023) provide insights into specific sectors like telecommunications and financial services. However, there is a gap in sector-specific research that includes healthcare, education, and government sectors, which are equally critical for comprehensive cybersecurity practices. Also, there is a lack of extensive studies on the regional disparities in the implementation and effectiveness of data privacy regulations, as noted in the ECOWAS Commission (2023) report. More research is needed to explore the harmonization of regulations across African countries and the impact of these disparities on multinational organizations operating within the continent.

By addressing these gaps, future research can provide a more comprehensive understanding of the effects of data privacy regulations on cybersecurity practices in Nigeria and Africa, ensuring that regulatory frameworks are both effective and adaptable to the unique challenges and opportunities within the region.

5. Summary of findings

The reviewed literature highlights the critical role of data privacy regulations in shaping cybersecurity practices across Nigeria and Africa. Institutional pressures, driven by regulatory frameworks such as Nigeria's NDPR and South Africa's POPIA, have compelled organizations to strengthen their cybersecurity measures to ensure compliance and legitimacy (Akinyede et al., 2021; Dlamini & Modise, 2022). However, challenges in enforcement, such as resource constraints and weak institutional capacity, hinder the effectiveness of these regulations in many African countries (Kamau, 2022). Public awareness has been shown to enhance cybersecurity behavior, but limited efforts in broad-based awareness campaigns reduce this potential (Toure et al., 2021). Additionally, while data privacy laws encourage technology adoption and investment in cybersecurity infrastructure, stringent regulations may stifle innovation, especially for tech startups (Ncube, 2020). Sectoral disparities and regional inconsistencies further complicate the harmonization and implementation of regulations across the continent (ECOWAS Commission, 2023). These findings underscore the need for a balanced, inclusive, and harmonized approach to data privacy regulations to ensure effective cybersecurity practices.

6. Conclusion

The literature reveals that data privacy regulations significantly influence cybersecurity practices in Nigeria and Africa. These regulations create institutional pressures that drive organizations to adopt stronger cybersecurity measures to ensure compliance and maintain legitimacy. However, the effectiveness of these regulations varies across countries and sectors, influenced by factors such as enforcement capabilities, public awareness, and the perceived utility of cybersecurity technologies. Challenges such as weak enforcement and the potential negative impact on innovation highlight the need for a balanced approach to regulatory frameworks. Overall, while data privacy regulations have generally improved cybersecurity practices, their full potential is often undermined by resource limitations and varying levels of implementation across the continent.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Since this study is based on secondary data, ethical concerns revolve around proper citation and acknowledgment of sources. The research adheres to ethical guidelines by ensuring that all reviewed literature is accurately referenced and that no intellectual property rights are violated.

Data availability

The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

Adediran, O. & Okon, I. (2023). “Challenges of data privacy enforcement in Nigeria: A regulatory perspective”. *Journal of Cybersecurity and Data Protection*. 5(2): 45-62.

Adeoye, A.A. & Adeoye, M.O. (2021). “Cybersecurity readiness in the healthcare sector: An assessment post-NDPR in Nigeria”. *African Journal of Science, Technology, Innovation and Development.* 13(4): 456-472. https://doi.org/10.1080/20421338.2021.1907218.

African Union Commission. (2022). “Assessing the effectiveness of data privacy regulations on cybersecurity across Africa”. *African Journal of Legal Studies*. 15(3): 200-220. https://doi.org/10.1163/17087384-2022AJLS045.

African Union. (2014). “African Union convention on cyber security and personal data protection”. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Akinyede, O.; Awodele, O. & Agbeyangi, A. (2021). “Awareness and compliance with Nigeria Data Protection Regulation among Nigerian organizations”. *Journal of Cyber Security Technology*. 5(2): 140-159. https://doi.org/10.1080/23742917.2021.1902094.

Aloamaka, P.C.A. (2023). “Data protection and privacy challenges in Nigeria: Lessons from other jurisdictions”. *UCC Law Journal*. 3(1): 281-321. https://doi.org/10.47963/ucclj.v3i1.1259.

Anderson, R. (2001). “Security engineering: A guide to building dependable distributed systems”. *IEEE Security & Privacy*. 1(1): 19-25. https://doi.org/10.1109/MC.2003.1146732.

Babalola, O. (2023). “Data protection and the right to privacy in Nigeria: A bibliography”. ssrn. https://ssrn.com/abstract=4625918.

Bello, I. & Yusuf, A. (2023). “Data privacy compliance and consumer trust in Nigerian e-commerce platforms”. *International Journal of Electronic Commerce Studies*. 14(1): 100-120. https://doi.org/10.7903/ijecs.2023.0009.

Bennett, N. (2025). “Large language models pose growing security risks”. *The Wall Street Journal*. https://www.wsj.com/articles/large-language-models-pose-growing-security-risks-f3c84ea9.

Bertino, E. & Sandhu, R. (2008). “Regulatory compliance in data management”. In *Encyclopedia of Database Systems* (pp. 2435-2439). Springer. https://doi.org/10.1007/978-0-387-39940-9_305.

Boateng, R.; Hinson, R.; Heeks, R. & Molla, A. (2022). “The impact of data protection laws on cybersecurity practices in Africa: A comparative study". *African Journal of Information Systems*. 14(3): 321-345. https://doi.org/10.1007/s10462-022-10072-3.

Bouke, M.A.; Abdullah, A.; ALshatebi, S.H.; El. Atigh, H. & Cengiz, K. (2023). "African union convention on cyber security and personal data protection: Challenges and future directions". *arXiv preprint arXiv*. 2307.01966. https://doi.org/10.48550/arXiv.2307.01966.

Chika, D.M. & Tochukwu, E.S. (2020). "An analysis of data protection and compliance in Nigeria". *International Journal of Research and Innovation in Social Science (IJRISS)*. 4(5). 377-382. https://www.researchgate.net/publication/342068885_An_Analysis_of_Data_Protection_and_Compliance_in_Nigeria.

Dlamini, S. & Modise, T. (2022). "Longitudinal assessment of POPIA's impact on cyber threats in South Africa". *Journal of Information Security and Applications*. 66: 102969. https://doi.org/10.1016/j.jisa.2022.102969.

ECOWAS Commission. (2023). "Harmonization of data privacy and cybersecurity regulations in West Africa: Progress and challenges". *Journal of West African Studies*. 8(2): 215-235. https://doi.org/10.1080/23774894.2023.2174927.

European Union. (2016). "General Data Protection Regulation (GDPR)". *Official Journal of the European Union*. L119: 1-88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

Goddard, M. (2017). "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". *International Journal of Law and Information Technology*. 25(3): 163-198. https://doi.org/10.1093/ijlit/eax003.

ISO. (2018). "ISO/IEC 27005: Information security risk management. International Organization for Standardization". https://www.iso.org/standard/75281.html.

Kamau, N. (2022). "Enforcement challenges in data privacy regulations: A case study of Kenya". *African Journal of Criminology and Justice Studies*. 15(2): 90-110. https://doi.org/10.31920/2050-4251/2022/15n2a6.

Kshetri, N. (2021). "The economics of personal data and cyber security". *IT Professional*. 23(3): 21-28. https://doi.org/10.1109/MITP.2021.3058985.

---------------. (2019). "Cybercrime and cybersecurity in Africa". *Journal of Global Information Technology Management*. 22(2): 77-81. https://doi.org/10.1080/1097198X.2019.1603527.

Mensah, C.A. & Osei, E.A. (2023). "Investment trends in cybersecurity post-data privacy regulation in Ghana's telecommunications sector". *Journal of Information, Communication and Ethics in Society*. 21(1): 100-120. https://doi.org/10.1108/JICES-05-2022-0042.

Mwangi, J. & Njenga, K. (2023). "Regulatory impact on cybersecurity incidents in Kenya's financial sector". *International Journal of Cyber Criminology*. 15(1): 75-94. https://doi.org/10.5281/zenodo.4727346.

NITDA: National Information Technology Development Agency. (2023). *Nigeria Data Protection Act 2023: Implications for organizations*. Abuja, Nigeria: NITDA.

---------------. (2019). "Nigeria data protection regulation". https://nitda.gov.ng/nigeria-data-protection-regulation-2019/.

NIST: National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042024.pdf.

---------------. (2020). "Risk management framework for information systems and organizations: A system lifecycle approach for security and privacy" (NIST Special Publication 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2.

---------------. (2018). "Risk management framework for information systems and organizations: A system lifecycle approach for security and privacy" (NIST Special Publication 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2.

Ncube, L. (2020). “The unintended consequences of data privacy regulations on tech startups in Zimbabwe”. *Journal of Business Venturing Insights*. 14: e00175. https://doi.org/10.1016/j.jbvi.2020.e00175.

Nte, N.D. & Teru V. (2022). “Intelligence education for national security and public safety policy: A comparative analysis of Nigeria, South Africa, and Indonesia”. *Lex Scientia Law Review*. 6(1): 187-218. http://dx.doi.org/10.15294/lesrev.v6i1.54431.

Okereafor, E.E. & Emembolu, I. (2020). “Cybersecurity practices in Nigerian organizations: A regulatory perspective”. *International Journal of Cybersecurity and Digital Forensics*. 9(1): 42-59. https://doi.org/10.17781/P002624.

Olawunmi, O. & Emejuo, C. (2021). “Nigeria data protection regulation”. https://nitda.gov.ng/nigeria-data-protection-regulation-2019/.

Oyewole, T. & Oduwole, A. (2022). “The impact of data protection regulations on cybersecurity practices in Nigeria”. *African Journal of Information Security*. 7(1): 89-104.

Parker, C. & Nielsen, V.L. (2017). “Compliance: 14 questions”. In C. Parker, C. Scott, N. Lacey, & J. Braithwaite (Eds.). *Regulating Law* (pp. 217–232). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199264070.003.0012.

Scholl, F. (2025). “Security concerns rise over Elon Musk's DOGE”. *CT Insider*. https://www.ctinsider.com/business/article/elon-musk-doge-digital-security-20175416.php.

Schwartz, P.M. & Solove, D.J. (2011). “The PII problem: Privacy and a new concept of personally identifiable information”. *New York University Law Review*. 86: 1814-1894. https://www.nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/.

Smith, J. (2020). “The impact of data protection regulations on organizational cybersecurity strategies”. *Cybersecurity Journal*. 35(2): 102-118. https://doi.org/10.1080/01436597.2020.1756745.

Solove, D.J. (2006). “A taxonomy of privacy”. *University of Pennsylvania Law Review*. 154(3): 477-564. https://doi.org/10.2307/40041279.

Statista. (2023). “Internet usage in Nigeria- statistics & facts”. https://www.statista.com/topics/2364/internet-usage-in-nigeria/.

Suchman, M.C. (1995). “Managing legitimacy: Strategic and institutional approaches”. *Academy of Management Review*. 20(3): 571-610. https://doi.org/10.5465/amr.1995.9508080331.

Toure, M.; Sagna, M. & Diop, D. (2021). “Data privacy awareness and cybersecurity behavior among West African internet users”. *Journal of Cyber Policy*. 6(2): 245-262. https://doi.org/10.1080/23738871.2021.1940842.

UNCTAD: United Nations Conference on Trade and Development. (2021). “Digital economy report 2021: Cross-border data flows and development”. https://unctad.org/webflyer/digital-economy-report-2021.

UNECA. (2020). *Cybersecurity and Data Protection in Africa: A Policy Handbook*. https://www.uneca.org/publications/cybersecurity-and-data-protection-africa-policy-handbook.

Voigt, P. & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7.

Wachter, S. (2018). “Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR”. *Computer Law & Security Review*. 34(3): 436-449. https://doi.org/10.1016/j.clsr.2018.05.010.