COMPARATIVE ANALYSIS OF LEGAL FRAMEWORK IN THE BAD AND THE GOOD OF CYBER TECHNOLOGY IN CHINA AND NIGERIA

OLUWASEUN, Ajoba[1]

Abstract

This study examined the legal frameworks governing cyber technology in two significant emerging economies: China and Nigeria. These countries represent distinct approaches to cybersecurity governance - China as a technological powerhouse with extensive regulatory control and Nigeria as Africa's largest economy striving to balance security imperatives with democratic values and developmental needs. The aim of this study is to presents a comprehensive comparative analysis of the legal frameworks governing cyber technology in China and Nigeria, examining both the positive aspects (the good) and problematic elements (the bad) inherent in each system. The study employs doctrinal legal research methodology, analyzing primary and secondary sources to evaluate the effectiveness, scope, and implications of cybersecurity laws in both jurisdictions. China's framework demonstrates comprehensive regulatory architecture with strong enforcement mechanisms but suffers from restrictive approaches and surveillance concerns. Nigeria's framework shows adaptive legislative modernization with rights-conscious provisions but faces significant implementation challenges and concerning surveillance provisions. The study found that while both countries have developed extensive legal frameworks, their approaches reflect different priorities: China prioritizes state security and comprehensive control, while Nigeria attempts to balance security needs with democratic values. The study recommends amongst others that there should be enhanced transparency and flexibility for China's framework, and an improved implementation capacity and rights safeguards for Nigeria's system. In conclusion, these findings contribute to understanding how emerging economies approach cybersecurity governance and the trade-offs between security, innovation, and individual rights in the digital age.

Keywords: Cybersecurity Law, Data Protection, Legal Framework, Comparative Analysis, China, Nigeria, Cyber Technology Regulation

Introduction

The emergence of cybersecurity as a critical governance issue reflects the increasing digitalization of economic and social activities worldwide.[2] International organizations, including the United Nations, International Telecommunication Union, and various regional bodies, have recognized cybersecurity as essential for sustainable development, economic prosperity, and national security.[3] However, the absence of binding international frameworks for cybersecurity governance has resulted in diverse national approaches that reflect different priorities, capabilities, and values.[4] The development of national cybersecurity frameworks has been influenced by several factors, including the level of technological development, threat perceptions, legal traditions, and political systems.[5] Advanced economies have generally focused on comprehensive regulatory frameworks that address multiple aspects of cyber governance, while developing countries often struggle with implementation capacity and resource constraints.[6]

[1] **OLUWASEUN, Ajoba**, a Legal Practitioner and Ph. D Scholar at Joseph Ayo Babalola University, Ikeji Arakeji, Tel: 08035788200

[2] A Murray and C Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power" (2002) 65 *Modern Law Review* 491, 495.

[3] International Telecommunication Union, Global Cybersecurity Index 2024 (Geneva, Switzerland: ITU Publications 2024) 8.

[4] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (Vienna, Austria: UNODC 2024) 18.

[5] D Svantesson, Cybersecurity Law (UK: Edward Elgar Publishing 2020) 67.

[6] ibid 72.

China's approach to cybersecurity governance has evolved significantly since the early 2000s, reflecting the country's rapid digital transformation and growing awareness of cyber threats.[7] The development of China's cybersecurity framework can be traced through several phases: initial focus on information security in the 1990s, comprehensive cybersecurity legislation in the 2010s, and the current phase of refined implementation and enforcement.[8] The establishment of the Cyberspace Administration of China (CAC) in 2014 marked a significant milestone in the country's cybersecurity governance, centralizing regulatory authority and providing institutional capacity for comprehensive oversight.[9] The subsequent enactment of the Cybersecurity Law in 2016, followed by the Data Security Law and Personal Information Protection Law in 2021, created what is commonly referred to as the "three-pillar system" of cyber governance.[10]

Nigeria's cybersecurity governance development reflects the challenges and opportunities facing African countries in the digital age.[11] The country's initial regulatory efforts focused primarily on telecommunications regulation and financial sector oversight, with cybersecurity considerations gradually integrated into broader regulatory frameworks.[12] The enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015 marked Nigeria's first comprehensive attempt to address cybercrime through dedicated legislation.[13] Subsequent developments, including the Nigeria Data Protection Regulation 2019 and the recent Data Protection Act 2023, demonstrate the country's evolving approach to cyber governance.[14] The establishment of the Nigeria Data Protection Commission as an independent regulatory body represents a significant milestone in the country's data protection regime.[15]

The digital revolution has fundamentally transformed the global landscape, creating unprecedented opportunities for economic growth, social interaction, and technological advancement while simultaneously generating complex security challenges that transcend national boundaries.[16] In response to these challenges, nations worldwide have developed comprehensive legal frameworks to govern cybersecurity and data protection, with varying degrees of success and different philosophical approaches to balancing security, privacy, and innovation.[17] This paper examines the legal frameworks governing cyber technology in two significant emerging economies: China and Nigeria. These countries represent distinct approaches to cybersecurity governance - China as a technological powerhouse with extensive regulatory control and Nigeria as Africa's largest economy striving to balance security imperatives with democratic values and developmental needs.[18] The comparative analysis focuses specifically on identifying and evaluating the positive aspects (the good) and problematic elements (the bad) within each legal framework.

[7] Segal, A. and Rosen, D., "China's Cyber Governance Model" (2023) 28 International Security Studies 67, 69.
[8] ibid 71.
[9] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)" (12 February 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii) accessed on 24th July 2025.
[10] ICLG, "Cybersecurity Laws and Regulations Report 2025 China" (6 November 2024) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.
[11] A Okunoye, "Evolution of Nigeria's Data Protection Regime" (2023) 12 *Nigerian Law Journal* 89, 91.
[12] ibid 93.
[13] Wigwe And Partners, "The Legal Framework for Cyber Crimes in Nigeria" (27 September 2024) https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 24th July 2025.
[14] ICLG, "Data Protection Laws and Regulations Report 2025 Nigeria" (21 July 2025) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.
[15] KPMG Nigeria, "The Nigeria Data Protection Act, 2023" (12 September 2023) https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023.html accessed 24 July 2025.
[16] International Telecommunication Union, 'Global Cybersecurity Index 2024' (Geneva, Switzerland: ITU Publications 2024) 15.
[17] United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (Vienna, Austria: UNODC 2024) 23.
[18] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (I)" (24 January 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(i) accessed 24th July 2025; ICLG, "Data Protection Laws and Regulations Report 2025 Nigeria" (21 July 2025) https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria accessed on 24th July 2025.

The significance of this comparative study lies in understanding how different legal traditions, political systems, and developmental priorities influence cybersecurity governance approaches.[19] China's comprehensive three-pillar system comprising the Cybersecurity Law, Data Security Law, and Personal Information Protection Law represents one of the world's most extensive regulatory frameworks for cyber governance.[20] Nigeria's recent legislative developments, including the Data Protection Act 2023 and the amended Cybercrimes Act 2024, demonstrate the challenges and opportunities facing developing countries in establishing effective cybersecurity governance.[21] The analysis reveals fundamental tensions between security and freedom, state control and individual rights, comprehensive regulation and implementation capacity, that characterize cybersecurity governance in the contemporary era. These tensions manifest differently in each jurisdiction, reflecting distinct political, economic, and social contexts that shape regulatory approaches and outcomes.

1.1 Research Purpose and Methodology

This study employs a qualitative research design using doctrinal legal research methodology. Doctrinal research involves systematic analysis of legal rules, principles, and frameworks through examination of primary and secondary sources.[22] This approach is appropriate for comparative legal analysis as it enables detailed examination of legal frameworks, their provisions, and their practical implications. The study relied on both primary and secondary sources of data. Primary Sources relied on are; Legislative texts including the Chinese Cybersecurity Law, Data Security Law, and Personal Information Protection Law, Nigerian Cybercrimes Act 2015 (as amended 2024) and Data Protection Act 2023, Regulatory Guidelines and Implementation Frameworks, Official Government Publications and Policy Documents while the Secondary Sources relied on are; Academic journals and scholarly articles, Professional legal analyses and commentary, International organization reports, Comparative law studies and policy analyses. The study employs comparative legal analysis methodology, systematically examining the legal frameworks of both countries to identify similarities, differences, strengths, and weaknesses. The analysis follows a structured approach like; systematic description of each framework's structure, scope, and key provisions, critical assessment of positive and negative aspects of each framework, systematic comparison of frameworks to identify patterns, differences, and implications, and development of recommendations based on identified strengths and weaknesses.

1.2 Research Problems and Limitations

Despite the increasing recognition of cybersecurity as a critical governance issue, there remains limited comparative analysis of how different legal frameworks address the inherent tensions between security, privacy, innovation, and development in the cyber domain. The proliferation of national cybersecurity frameworks has created a complex landscape where different approaches yield varying outcomes in terms of effectiveness, rights protection, and economic impact.[23] China and Nigeria represent two distinct approaches to cybersecurity governance that warrant detailed comparative analysis. China's comprehensive and state-centric approach contrasts sharply with Nigeria's attempts to balance security needs with democratic values and developmental priorities.[24] However, both frameworks exhibit positive elements that contribute to cybersecurity objectives as well as problematic aspects that raise concerns about rights protection, implementation effectiveness, and long-term sustainability.[25]

---

[19] D Svantesson, *Cybersecurity Law* (UK: Edward Elgar Publishing 2020) 45.

[20] ICLG, "Cybersecurity Laws and Regulations Report 2025 China" (6 November 2024) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china accessed on 24th July 2025.

[21] NALTF, "Nigeria's Cybercrime Reform" https://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on 24th July 2025.

[22] M Pearson, Legal Research Methodology, 4th edn. (UK: LexisNexis Publication 2018) 67.

[23] Svantesson, D., Cybersecurity Law (UK: Edward Elgar Publishing 2020) 89.

[24] Future of Privacy Forum, "Nigeria's New Data Protection Act, Explained" https://fpf.org/blog/nigerias-new-data-protection-act-explained/ accessed on 24th July 2025.

[25] China Briefing, "China's Cybersecurity Law Amendments 2025: Second Draft Highlights" (1 April 2025) https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/ accessed on 24th July 2025.

The lack of systematic comparative analysis of these frameworks limit understanding of the trade-offs inherent in different approaches to cybersecurity governance. This knowledge gap is particularly significant for other emerging economies seeking to develop effective cybersecurity frameworks that balance competing priorities and constraints.[26] Furthermore, the rapid evolution of cyber threats and technologies requires continuous evaluation of existing frameworks to identify strengths and weaknesses that inform future policy development.[27] Flowing from the above mentioned problems, this study attempted to resolve the following objectives; examined the structure, scope, and key provisions of cybersecurity legal frameworks in China and Nigeria; identified and analysed the positive aspects (the good) of each legal framework, including their contributions to cybersecurity, data protection, and technological governance; critically evaluated the problematic elements (the bad) within each framework, including their limitations, adverse effects, and implementation challenges; conducted a comparative analysis of both frameworks, highlighting similarities, differences, and the factors that influence their respective approaches; and made a contribution to the broader understanding of cybersecurity governance approaches in emerging economies and their implications for policy development.

It is worthy of note that several limitations affected this study such as Language Barriers: Some Chinese regulatory documents may be available only in Chinese, potentially limiting access to certain primary sources. Also, Rapid Regulatory Changes: Both countries continue to update their frameworks, which may affect the currency of some analyses; Implementation Data: Limited availability of comprehensive implementation data may affect assessment of practical effectiveness, and Cultural Context: Understanding the full implications of legal frameworks requires deep cultural and political context that may be difficult to capture fully in comparative analysis

2.0. Theoretical Frameworks

This study employs **regulatory theory** as its primary theoretical framework, drawing on Baldwin, Cave, and Lodge's comprehensive analysis of regulation and regulatory systems.[28] Regulatory theory provides analytical tools for understanding how different regulatory approaches address market failures, coordinate behavior, and achieve policy objectives in complex environments. The framework identifies several key dimensions of regulatory analysis relevant to cybersecurity governance like; understanding what each framework seeks to achieve, examining the mechanisms used to achieve the objectives, institutional arrangements such as analyzing the organizational structures and processes, evaluating the outcomes against the objectives, legitimacy and accountability by assessing democratic oversight and stakeholder participation.

State capacity theory, as developed by Fukuyama and others, provides important insights into understanding the differential effectiveness of cybersecurity frameworks.[29] This theory examines how state capabilities - including institutional capacity, technical expertise, and resource availability - influence regulatory effectiveness. The theory is particularly relevant for understanding the differences between China and Nigeria's frameworks, as it helps explain how state capacity constraints affect implementation and enforcement of cybersecurity regulations.

[26] O Adebayo, "Implementation Challenges in Nigeria's Cybersecurity Framework" (2024) 18 *African Journal of Legal Studies* 123, 125.

[27] International Telecommunication Union, Global Cybersecurity Index 2024 (Geneva, Switzerland: ITU Publications 2024) 34.

[28] R Baldwin, M Cave, and M Lodge, Understanding Regulation: Theory, Strategy, and Practice (2nd edn, Oxford University Press 2012) 89.

[29] F Fukuyama, Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy (Farrar, Straus and Giroux 2014) 234.

Watson's legal transplant theory provides insights into how legal frameworks develop through borrowing and adaptation from other jurisdictions.[30] This theory is relevant for understanding how both China and Nigeria have adapted international best practices and models to their domestic contexts. The theory helps explain both successful adaptations and implementation challenges that arise when legal frameworks are transplanted across different political, economic, and cultural contexts.

3.0. Literature Review and Comparative Insights

The academic literature on cybersecurity governance has developed several theoretical frameworks for understanding how States approach cyber regulation. Murray and Scott identify three primary models: market-based regulation, state-centric regulation, and hybrid approaches that combine public and private governance mechanisms.[31] These models provide analytical frameworks for understanding the different approaches adopted by China and Nigeria. Lessig's "Code is Law" theory offers another important perspective, suggesting that technological architectures themselves serve as regulatory mechanisms alongside legal frameworks.[32] This perspective is particularly relevant for understanding how China's comprehensive approach integrates legal requirements with technological controls to achieve cybersecurity objectives.

Comparative analysis of cybersecurity frameworks has received increasing academic attention. Svantesson's work on cybersecurity law provides comprehensive analysis of different national approaches, identifying common challenges and diverse solutions.[33] However, limited attention has been paid to the specific comparison between China and Nigeria's frameworks. Bradford's "Brussels Effect" theory, which examines how comprehensive regulatory frameworks can influence global standards, provides insights into how China's extensive cybersecurity regime may affect international norms and practices.[34] This perspective is relevant for understanding the broader implications of China's regulatory approach. Academic analysis of China's cybersecurity framework has focused primarily on its comprehensive nature and state-centric approach. Segal and Rosen provide detailed analysis of China's cyber governance model, highlighting its emphasis on sovereignty and state control.[35] However, most literature focuses on the framework's restrictive aspects without systematically examining its positive contributions to cybersecurity.

Recent scholarship by Liao and others has begun to examine the implementation challenges and practical effects of China's cybersecurity laws, providing insights into the gap between regulatory ambitions and operational realities.[36] This literature suggests that China's framework, while comprehensive, faces significant implementation complexities. Academic literature on Nigeria's cybersecurity framework is more limited, reflecting the relatively recent development of comprehensive legal frameworks in the country. Okunoye and others have examined the evolution of Nigeria's data protection regime, highlighting both progress and challenges.[37] However, comprehensive comparative analysis remains limited.

Recent work by Adebayo and others has examined the implementation challenges facing Nigeria's cybersecurity framework, identifying resource constraints and capacity limitations as significant barriers to effectiveness.[38] This literature provides important context for understanding the practical challenges facing

[30] A Watson, Legal Transplants: An Approach to Comparative Law (2nd edn, University of Georgia Press 1993) 45.
[31] A Murray, and C Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power" (2002) 65 *Modern Law Review* 491, 498.
[32] L Lessig, Code: Version 2.0 (Basic Books 2006) 78.
[33] Svantesson, D., Cybersecurity Law (UK: Edward Elgar Publishing 2020) 123.
[34] A Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020) 156.
[35] A Segal, and D Rosen, "China's Cyber Governance Model" (2023) 28 *International Security Studies* 67, 74.
[36] R Liao, "Implementation Challenges in China's Cybersecurity Framework" (2024) 45 *Computer Law & Security Review* 105, 108.
[37] A Okunoye, "Evolution of Nigeria's Data Protection Regime" (2023) 12 *Nigerian Law Journal* 89, 97.
[38] O Adebayo, "Implementation Challenges in Nigeria's Cybersecurity Framework" (2024) 18 *African Journal of Legal Studies* 123, 130.

developing countries in cybersecurity governance. The existing literature reveals several gaps that this study addressed. First, there is limited systematic comparative analysis of China and Nigeria's cybersecurity frameworks. Second, most existing literature focuses on either positive or negative aspects of frameworks without comprehensive evaluation of both. Third, limited attention has been paid to the specific challenges facing emerging economies in balancing cybersecurity with development objectives.

4. 0. The Good: Positive Aspects of Legal Frameworks

China's cybersecurity legal framework demonstrates remarkable comprehensiveness through its three-pillar system comprising the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL).[39] This systematic approach creates a robust regulatory ecosystem that addresses different aspects of cyber governance in a coordinated manner. The Network Data Security Management Regulations, effective January 1, 2025, further strengthen coordination among these legal frameworks.[40] The systematic division of regulatory focus prevents gaps and overlaps that plague less organized legal systems. The CSL addresses network security and critical information infrastructure protection, the DSL focuses on data security and classification, while the PIPL governs personal information protection.[41] This architectural approach ensures comprehensive coverage while maintaining regulatory clarity.

China's framework includes robust enforcement mechanisms with significant penalties designed to create effective deterrence.[42] The 2025 amendments to the CSL introduce stricter penalties that align with those in the DSL and PIPL, creating penalty harmonization across the three laws.[43] The amendments introduce graded penalties based on violation severity, with fines reaching up to 10% of annual revenue for serious violations.[44] The enforcement system operates through multiple regulatory bodies with specialized mandates. The Cyberspace Administration of China (CAC) serves as the primary cybersecurity regulator, while sector-specific authorities handle industry-specific requirements.[45] This multi-layered enforcement approach ensures comprehensive oversight across different sectors and violation types.

The framework provides clear hierarchical protection for different categories of data, with specific provisions for important data and critical information infrastructure.[46] The Network Data Security Management Regulations establish detailed criteria for identifying important data and require local authorities to establish catalogues of important data for relevant industries and sectors.[47] This systematic approach helps businesses understand their obligations and implement appropriate protection measures. The classification system provides predictability and enables risk-based approaches to data protection that balance security needs with operational efficiency. Despite its restrictive reputation, China's framework includes provisions supporting international cooperation within security parameters. The regulations provide

[39] ICLG, "Cybersecurity Laws and Regulations Report 2025 China" (6 November 2024) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.

[40] China Briefing, "China Issues New Regulations on Network Data Security Management" (2 October 2024) https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/ accessed on 24th July 2025.

[41] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (I)" (24 January 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(i) accessed 24th July 2025

[42] China Briefing, "China's Cybersecurity Law Amendments 2025: Second Draft Highlights" (1 April 2025) https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/ accessed on 24th July 2025.

[43] ibid.

[44] ibid.

[45] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)" (12 February 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii) accessed on 24th July, 2025.

[46] ICLG, "Cybersecurity Laws and Regulations Report 2025 China" (6 November 2024) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.

[47] China Briefing, "China Issues New Regulations on Network Data Security Management" (2 October 2024) https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/ accessed on 24th July 2025.

pathways for legitimate cross-border data transfers through security assessments, standard contracts, and certification mechanisms.[48] The framework recognizes the importance of international business while maintaining security oversight.

Nigeria has demonstrated remarkable legislative agility in updating its cyber technology framework. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 significantly strengthened the original 2015 Act by addressing evolving cyber threats and expanding the scope of covered offenses.[49] This responsiveness to changing threat landscapes demonstrates effective legislative adaptation. The Nigeria Data Protection Act 2023 (NDPA) represents a major advancement in the country's data protection regime.[50] The Act establishes a comprehensive legal framework that aligns with international standards while considering local contexts and development needs, demonstrating Nigeria's commitment to global best practices. The NDPA creates an independent regulatory body, the Nigeria Data Protection Commission (NDPC), demonstrating Nigeria's commitment to establishing proper oversight mechanisms free from direct government interference.[51] This independence is crucial for building public trust and ensuring fair enforcement of data protection laws. The framework includes innovative concepts such as "data controllers and processors of major importance," reflecting a tiered approach similar to international frameworks like the EU's Digital Services Act.[52] This demonstrates Nigeria's effort to learn from global experiences while adapting regulations to local conditions.

Nigeria's framework attempts to balance security needs with democratic values and individual rights protection.[53] The NDPA includes comprehensive rights for data subjects, including rights to access, correction, and deletion of personal data.[54] The framework provides clear consent mechanisms and restricts processing without lawful basis. The data protection framework includes provisions for cross-border data transfers with adequate protection mechanisms, balancing data protection requirements with the needs of international business and economic development.[55] This approach recognizes Nigeria's position as an emerging economy requiring international cooperation and investment.

Nigeria's approach demonstrates flexibility through implementation guidance. The General Application and Implementation Directive (GAID) issued by the NDPC provides additional clarification and practical guidance for compliance.[56] This flexible approach allows for adaptive implementation as the regulatory framework matures. The framework includes graduated enforcement approaches, with different requirements for different sizes and types of organizations.[57] This recognition of capacity differences among businesses demonstrates practical regulatory design that considers implementation realities.

---

[48] Hunton, "China Released Regulations on Administration of Network Data Security to Further Implement Cybersecurity and Protection of Personal Information" https://www.hunton.com/privacy-and-information-security-law/china-released-regulations-on-administration-of-network-data-security-to-further-implement-cybersecurity-and-protection-of-personal-information accessed on 24th July 2025.

[49] NALTF, "Nigeria's Cybercrime Reform" http://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on 22nd October 2025

[50] ICLG, "Data Protection Laws and Regulations Report 2025 Nigeria" (21 July 2025) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.

[51] KPMG Nigeria, "The Nigeria Data Protection Act, 2023" (12 September 2023) https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023.html accessed 24 July 2025.

[52] Future of Privacy Forum, "Nigeria's New Data Protection Act, Explained" https://fpf.org/blog/nigerias-new-data-protection-act-explained/ accessed 24 July 2025.

[53] NALTF, "Nigeria's Cybercrime Reform" http://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on 24th October 2025

[54] Securiti, "An Overview of Nigeria's Data Protection Act, 2023" (16 June 2025) https://securiti.ai/overview-of-nigeria-data-protection-act/ accessed on 24th July 2025.

[55] ibid.

[56] ICLG, "Data Protection Laws and Regulations Report 2025 Nigeria" (21 July 2025) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/Nigeria, accessed on 24th July 2025.

[57] Hogan Lovells, "Key Changes brought by the Nigerian Data Protection Act, 2023" https://www.hoganlovells.com/en/publications/key-changes-brought-by-the-nigerian-data-protection-act-2023 accessed on 24th July 2025.

5.0. The Bad: Problematic Aspects of Legal Frameworks

China's cyber technology framework suffers from excessively broad interpretations of national security and public interest that can restrict legitimate business activities and technological innovation.[58] The concept of "national security" is often applied expansively, creating uncertainty for businesses about what activities might trigger regulatory scrutiny. The data localization requirements and extensive cross-border transfer restrictions can significantly impede international business operations and limit technological advancement.[59] These restrictions often lack clear criteria and can be applied arbitrarily, creating compliance uncertainty for multinational companies operating in China. The framework grants extensive surveillance powers to authorities, raising serious concerns about privacy rights and business confidentiality.[60] The Cybersecurity Law allows authorities to access and inspect business data and systems under broad circumstances, often without clear judicial oversight mechanisms. The requirement for cybersecurity reviews of foreign technology products and services in critical sectors reflects a protectionist approach that may limit technological advancement and international cooperation.[61] These reviews can be used to exclude foreign competitors and protect domestic technology companies, potentially stifling innovation through reduced competition.

The enforcement mechanism, while robust, lacks transparency in decision-making processes.[62] Regulatory decisions are often made without clear explanation of reasoning or adequate opportunity for affected parties to present their cases. This opacity creates uncertainty and makes it difficult for businesses to predict regulatory outcomes. The appeals process for regulatory decisions is limited, with few effective mechanisms for challenging adverse regulatory determinations.[63] This lack of due process protections can result in arbitrary enforcement and unfair treatment of businesses, particularly foreign companies operating in China. The complex regulatory requirements impose significant compliance costs that disproportionately affect smaller enterprises and foreign companies.[64] The multiple reporting requirements, technical standards, and certification processes create substantial administrative burdens that may discourage innovation and entrepreneurship. The requirement for local data storage and processing forces companies to duplicate infrastructure and increases operational costs significantly.[65] These requirements may compromise global efficiency and integration of business operations, particularly for multinational companies.

Nigeria's primary challenge lies in the significant gap between comprehensive legislation and effective implementation.[66] The Nigerian Computer Emergency Response Team (ngCERT) and other enforcement agencies often lack sufficient resources, technical expertise, and infrastructure to address the volume and sophistication of cyber threats effectively. The lack of adequate funding for cybersecurity initiatives hampers effective implementation of the legal framework.[67] This resource constraint limits the government's ability

[58] China Briefing, "China Cybersecurity Regulations - What Does the Draft Regulation Say?" (5 September 2024) https://www.china-briefing.com/news/china-cybersecurity-regulations-what-do-the-new-regulations-say/ accessed on 24th July 2025.

[59] ibid.

[60] China Briefing, "China's Cybersecurity Law Amendments 2025: Second Draft Highlights" (1 April 2025) https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/ accessed on 24th July 2025.

[61] ibid.

[62] Two Birds, "China Cybersecurity and Data Protection: Monthly Update - December 2024 Issue" (23 December 2024) https://www.twobirds.com/en/insights/2024/china/china-cybersecurity-and-data-protection-monthly-update---december-2024-issue accessed on 24th July 2025.

[63] Chambers and Partners, "Cybersecurity 2024 - China" https://practiceguides.chambers.com/practice-guides/cybersecurity-2024/china/trends-and-developments accessed 24 July 2025.

[64] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)" (12 February 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii) accessed on 28th July, 2025.

[65] Wigwe And Partners, "The Legal Framework for Cyber Crimes in Nigeria" (27 September 2024) https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 24th July, 2025.

[66] Wigwe And Partners, "The Legal Framework for Cyber Crimes In Nigeria" (27 September 2024) https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 24th July, 2025.

[67] ibid.

to build necessary technical capabilities and train enforcement personnel adequately, creating significant implementation gaps. The 2024 amendment to the Cybercrimes Act introduces problematic surveillance provisions that grant security agencies authority to intercept communications in "urgent" cases without court orders.[68] This provision lacks clear definition of what constitutes "urgent" circumstances and provides insufficient safeguards against abuse. The requirement for telecom companies to retain user data for extended periods raises serious concerns about mass surveillance and privacy rights.[69] Given Nigeria's history of human rights challenges and concerns about government overreach, these provisions create significant risks for individual privacy and democratic freedoms.

The criminalization of "false" or "misleading" posts in the amended Cybercrimes Act has been criticized as potentially stifling freedom of expression and legitimate criticism.[70] The broad and vague nature of these provisions creates risks of arbitrary enforcement against journalists, activists, and ordinary citizens exercising their constitutional rights. The lack of clear definitions and safeguards for determining what constitutes "false" or "misleading" information creates potential for abuse and selective enforcement.[71] This vagueness particularly concerns civil society organizations working on governance and human rights issues. Enforcement of cybersecurity laws in Nigeria remains inconsistent, with some high-profile cases receiving attention while many violations go unaddressed.[72] While some institutions have paid substantial fines for data privacy violations, many smaller violations escape enforcement due to limited regulatory capacity. The technical sophistication required for effective cybersecurity enforcement often exceeds the current capabilities of Nigerian enforcement agencies.[73] This capacity gap means that sophisticated cybercriminals can operate with relative impunity while less technically savvy violators face prosecution, creating enforcement inequities.

6.0. Comparative Analysis and Discussion

The fundamental difference between China and Nigeria's frameworks lies in their underlying regulatory philosophies. China's approach prioritizes state security and comprehensive control, reflecting its authoritarian political system and emphasis on social stability.[74] Nigeria's framework attempts to balance security needs with democratic values and individual rights protection, reflecting its federal democratic system and constitutional commitments to human rights.[75] This philosophical difference manifests in specific regulatory choices. China's framework grants extensive powers to regulatory authorities with limited judicial oversight, while Nigeria's framework includes more procedural safeguards and rights protections, though recent amendments have introduced concerning surveillance provisions.[76] China demonstrates superior implementation capacity through adequate resources, technical capabilities, and institutional coordination.[77] The country's investment in cybersecurity infrastructure and personnel enables effective enforcement of its comprehensive regulatory requirements. However, this effectiveness comes with concerns about arbitrariness and lack of transparency in enforcement processes.

---

[68] NALTF, "Nigeria's Cybercrime Reform" http://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on 24th October 2025

[69] ibid.

[70] ibid.

[71] ibid.

[72] Mondaq, "Understanding the Nigeria Data Protection Act 2023: Obligations of Digital Platforms And Businesses" (29 February 2024) https://www.mondaq.com/nigeria/privacy-protection/1430338/understanding-the-nigeria-data-protection-act-2023-obligations-of-digital-platforms-and-businesses accessed on 24th July 2025.

[73] LegalDigitalNG, "Cybersecurity Laws in Nigeria: A Comprehensive Guide for Businesses Going Digital in 2025" (5 February 2025) https://legaldigitalng.com/cybersecurity-laws-in-nigeria-a-comprehensive-guide-for-businesses-going-digital-in-2025/ accessed on 24th July 2025.

[74] A Segal, and D Rosen, "China's Cyber Governance Model" (2023) 28 *International Security Studies* 67, 76.

[75] Future of Privacy Forum, "Nigeria's New Data Protection Act, Explained" https://fpf.org/blog/nigerias-new-data- protection-act-explained/ accessed 24 July 2025.

[76] ibid. (n 68); ibid. (n 60).

[77] Two Birds, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)" (12 February 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii) accessed on 24th July, 2025.

Nigeria faces significant implementation challenges due to resource constraints and limited technical capacity.[78] While the country has developed comprehensive legal frameworks, the gap between regulatory ambitions and implementation capabilities limits effectiveness. This capacity constraint affects both cybersecurity protection and rights enforcement. The frameworks differ significantly in how they balance security needs with individual rights and business interests. China's framework prioritizes security and state interests, often at the expense of individual privacy and business autonomy.[79] This approach may provide greater security but raises concerns about surveillance and authoritarian control. Nigeria's framework generally attempts to maintain better balance between security and rights, though recent amendments introduce concerning surveillance provisions.[80] The framework includes more robust procedural protections and rights safeguards, reflecting democratic governance principles. Both frameworks significantly impact economic activities and technological innovation, but in different ways. China's comprehensive approach provides regulatory certainty for domestic businesses but can restrict international cooperation and limit competition.[81] The extensive requirements may also discourage foreign investment and technological transfer.

Nigeria's framework aims to support economic development while maintaining security, but implementation challenges can create uncertainty for businesses.[82] The inconsistent enforcement and capacity limitations may undermine business confidence while failing to provide adequate security protection. China's framework includes provisions for international cooperation but within strict sovereignty constraints.[83] The emphasis on data localization and extensive transfer restrictions can limit international business operations and cooperation on cybersecurity matters. Nigeria's framework is more open to international cooperation and includes provisions facilitating cross-border business operations.[84] However, implementation challenges may limit the country's ability to participate effectively in international cybersecurity cooperation initiatives.

7.0. Conclusion and Recommendations

In conclusion, this study revealed the following findings and implications like;

Regulatory Comprehensiveness: Both countries have developed comprehensive legal frameworks, but China's systematic three-pillar approach provides more coordinated coverage than Nigeria's evolving framework.

Implementation Effectiveness: China demonstrates superior implementation capacity and enforcement effectiveness, while Nigeria faces significant capacity constraints that limit framework effectiveness.

Rights Protection: Nigeria's framework generally provides better protection for individual rights and democratic values, though recent amendments introduce concerning surveillance provisions similar to those in China's framework.

[78] Wigwe And Partners, "The Legal Framework for Cyber Crimes in Nigeria" (27 September 2024) https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 24th July, 2025.

[79] China Briefing, "China's Cybersecurity Law Amendments 2025: Second Draft Highlights" (1 April 2025) https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/ accessed on 24th July 2025.

[80] NALTF, "Nigeria's Cybercrime Reform" http://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on 24th October 2025

[81] China Briefing, "China Cybersecurity Regulations - What Does the Draft Regulation Say?" (5 September 2024) https://www.china-briefing.com/news/china-cybersecurity-regulations-what-do-the-new-regulations-say/ accessed on 24th July 2025.

[82] Mondaq, "Understanding the Nigeria Data Protection Act 2023: Obligations Of Digital Platforms And Businesses" (29 February 2024) https://www.mondaq.com/nigeria/privacy-protection/1430338/understanding-the-nigeria-data-protection-act-2023-obligations-of-digital-platforms-and-businesses accessed on 24th July 2025.

[83] Hunton, "China Released Regulations on Administration of Network Data Security to Further Implement Cybersecurity and Protection of Personal Information" https://www.hunton.com/privacy-and-information-security-law/china-released-regulations-on-administration-of-network-data-security-to-further-implement-cybersecurity-and-protection-of-personal-information accessed on 24th July 2025.

[84] Securiti, "An Overview of Nigeria's Data Protection Act, 2023" (16 June 2025) https://securiti.ai/overview-of-nigeria-data-protection-act/ accessed on 24th July 2025.

Economic Impact: Both frameworks significantly impact business operations, but China's restrictive approach may limit international cooperation while Nigeria's implementation challenges create uncertainty.
Innovation Effects: China's comprehensive control may provide stability but can restrict innovation through extensive regulations, while Nigeria's capacity limitations may fail to provide adequate protection for technological development.

The findings have several theoretical implications for understanding cybersecurity governance:
The comparison confirms the critical importance of state capacity in determining regulatory effectiveness, as demonstrated by the implementation gaps in Nigeria's framework.
The analysis reveals fundamental trade-offs between comprehensiveness and flexibility, security and rights, that characterize cybersecurity governance.

Context Dependency: The different approaches reflect how political, economic, and social contexts shape regulatory frameworks and their implementation.
Development Challenges: The Nigerian case illustrates the particular challenges facing developing countries in establishing effective cybersecurity governance while maintaining democratic values. The findings have important implications for understanding cybersecurity governance approaches in emerging economies and provide insights for policy development in other jurisdictions facing similar challenges. The study demonstrates that while comprehensive legal frameworks are necessary for effective cybersecurity governance, they are insufficient without adequate implementation capacity, institutional coordination, and careful attention to balancing competing values and interests. Future research should examine the implementation outcomes of these frameworks over time, assess their effectiveness in addressing evolving cyber threats, and explore how different approaches to cybersecurity governance affect innovation, economic development, and democratic governance. The rapidly evolving nature of cyber threats and technologies ensures that both countries will need to continue adapting their frameworks, providing ongoing opportunities for comparative analysis and learning.

The significance of this comparative analysis extends beyond the specific cases of China and Nigeria to contribute to broader understanding of how different political, economic, and social contexts shape cybersecurity governance approaches. As more countries develop comprehensive cybersecurity frameworks, the lessons learned from this analysis can inform policy development and help countries navigate the complex trade-offs inherent in cybersecurity governance. Ultimately, the goal of cybersecurity governance should be to create frameworks that effectively protect against cyber threats while preserving the benefits of digital innovation, international cooperation, and democratic values that are essential for sustainable development in the digital age. Both China and Nigeria continue to evolve their approaches, and their experiences provide valuable insights for the ongoing global effort to develop effective, rights-respecting, and developmentally appropriate cybersecurity governance frameworks.