# AN ANALYSIS OF THE EFFECTIVENESS OF CYBERCRIME LAWS IN NIGERIA: CHALLENGES AND SOLUTIONS

**Peace Ngozi OSAMOR**
**LAW2002943**

**FACULTY OF LAW**
**UNIVERSITY OF BENIN**
**BENIN CITY, NIGERIA**

**NOVEMBER, 2025**

# AN ANALYSIS OF THE EFFECTIVENESS OF CYBERCRIME LAWS IN NIGERIA: CHALLENGES AND SOLUTIONS

**Peace Ngozi OSAMOR**
**LAW2002943**

**BEING A PROJECT WORK SUBMITTED TO THE FACULTY OF LAW, UNIVERSITY OF BENIN, BENIN CITY, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF LAW**

**NOVEMBER, 2025**

## CERTIFICATION

I Peace Ngozi OSAMOR (Miss.) with matriculation number LAW2002943 hereby certify that apart from referenced' works which have been duly acknowledged, the entire work is a product of my research, and this project has neither in whole nor in part been presented for another degree elsewhere.

_____

**Peace Ngozi OSAMOR (Miss)**
**(**LAW2002943**)**

## APPROVAL

This is to certify that this project was carried out and completed by **Peace Ngozi OSAMOR** with Matriculation Number LAW2002943 in partial fulfillment of the requirements for the award of Bachelor of Law (LLB.) Degree, University of Benin.

**MRS NKECHI M. ALLI**
**PROJECT SUPERVISOR** _____ **SIGNATURE AND DATE**

**DR. OBIAGELI OSUJI**
**PROJECT COORDINATOR** _____ **SIGNATURE AND DATE**

**PROF. BRIGHT BAZUAYE**
**DEAN, FACULTY OF LAW** _____ **SIGNATURE AND DATE**

## DEDICATION

This project is dedicated to my parents, Mr. and Mrs. Felix D. Osamor. Your love, care, unwavering devotion and continuous support have been a great source of strength for me throughout this journey. For all the sacrifices which you have both made to get me to this point, for your love that knows no bounds and for your unshakeable faith in me, I am eternally grateful.

## ACKNOWLEDGEMENTS

My profound appreciation goes to God Almighty for His grace towards my life throughout my academic pursuit in University of Benin. I would like to extend my sincerest gratitude to my project supervisor, Mrs Nkechi Magdalene Alli, whose patience, guidance, accessibility and unwavering support has played a huge role in the successful completion of this project. I also want to thank my Dean, Professor Bright Bazuaye and other lecturers who have impacted my life tremendously, most especially Professor Michael Attah, Dr. Jacob Garuba and Dr. Sunday Omokhudu Daudu. For your kindness and your thoroughness in ensuring I leave the faculty of law, a more grounded individual than when I came in, I'm grateful.

My heartfelt gratitude also goes to my family. To my super daddy, Mr. Felix Osamor, thank you for your love, support, prayers and constant motivation from kindergarten till this moment; I'm eternally grateful daddy. To my mum, Mrs. Lucy Osamor, thank you ma mere; thank you for everything. And to my sister, Cherish, my smallie, thank you for always supporting me emotionally; you're a gift I'll always appreciate.

I would also love to sincerely thank my friends, Osilamah Lauretta "Lorito" and Oni-Ojo Neosa. Thank you both for being great friends.

To my classmates, the great legal luminaries, I'm happy I got to do this journey with you all. Thank you to Obikwere Prosper, Areghe Phoebe, Ididi Joshua, Ekule Marvellous and all other classmates who made my job as classrep easier in one way or the other.

Last but not least, thank you to my very own person, Mr Jude Chiedozie Ijeh; you deserve a paragraph of your own. Thank you for supporting me throughout this journey and just being a great friend.

Finally, my deepest thanks go to God Almighty whose grace, mercy and protection has sustained me throughout this journey. I would not have what it takes to see this through without God and for this I'm grateful, now and always.

## TABLE OF CONTENTS

**Table of Cases**

*Danfulani v. Economic and Financial Crimes Commission* (2016) 1 NWLR (Pt 1493) 223 scirp.org+2ace.soas.ac.uk+2

*Dasuki v. Federal Republic of Nigeria* (2018) 10 NWLR (Pt 1627) 320 ace.soas.ac.uk+1
*Yanaty Petrochemical Ltd v. Economic and Financial Crimes Commission* (2017) 3 NWLR (Pt 1552), Supreme Court. ace.soas.ac.uk+1
*Economic and Financial Crimes Commission v. Diamond Bank Plc.* (2018) 8 NWLR (Pt 1620) 61. (cited in ACE working paper) ace.soas.ac.uk+1

*Alao v. Federal Republic of Nigeria* (2018) 10 NWLR (Pt 1627) 284. ace.soas.ac.uk
*Auwalu v. Federal Republic of Nigeria* (2018) 8 NWLR (Pt 1620) 1. ace.soas.ac.uk+1
*Ihenacho v. Nigerian Police Force* (2017) 12 NWLR (Pt 1580) 423. ace.soas.ac.uk
*Okoye v. Santili* (1994) 4 NWLR (Pt 338) 256. ace.soas.ac.uk
*Olagunju v. Federal Republic of Nigeria* (2018) 10 NWLR (Pt 1627) 272. ace.soas.ac.uk
*Osahon v. Federal Republic of Nigeria* (2003) 16 NWLR (Pt 845) 89. ace.soas.ac.uk
*PML Securities Company Limited v. Federal Republic of Nigeria* (2015) 4 NWLR (Pt 1450) 551. ace.soas.ac.uk

*Dr. Imoro Kubor v. Seriake Henry Dickson* (2013) 4 NWLR (Pt. 1345) 534

Julius v. Federal Republic of Nigeria (2021) LPELR-54201 (CA) (2021)

*Solomon Okedara v. Attorney General of the Federation* — Court of Appeal (2019), CA/L/174/18.

Alhaji Musa Sani v. The State (2015)**,** SC.36/2013 Supreme Court.

*Online Policy Group v. Diebold, Inc.**,** No. C 03- 03899, 337 F. Supp.* 2d 1195 (N.D. Cal. 2003).

*Intel Corp. v. Hamidi**, 30 Cal. 4th* 1342, 1350 (2003).

Oluseun Olumide Fadele, Esq. v. Economic and Financial Crimes Commission, FCT/HC/GWD/CV/126/21 (High Court, FCT, Abuja, 4 April 2022).

Federal Republic of Nigeria v. Emmanuel Nwude & Others (2005) 14 NWLR (Pt. 1000) 1.

*MADUKA & ORS v. IGP & ORS* (2020), LCN/14264(CA)

AUWAL v. Federal Republic of Nigeria **(2022), (2022)LCN/16319(CA)**

*Federal Republic of Nigeria v. Wilfred Fajemisin* Feb 21, 2022, 19 NWLR (Pt. 680) 1375

***Edward Nathan Sonnenberg Inc v. Hawarden* [2024] ZASCA 90**

*Oluseun Olumide Fadele, Esq. v. Economic and Financial Crimes Commission,* (2022) FCT/HC/GWD/CV/126/21.

*Osahon v. Federal Republic of Nigeria* (2003) 16 NWLR (Pt 845) 89.

*Nwankwoala* v. *Federal Republic of Nigeria* (2018) 14 NWLR (Pt. 1639) 459 at 482

*Federal Republic of Nigeria v. Justice Mohammed Yunusa* & 1 other (2018) FHC/L/CS/ 714/2015, FHC/L/CS/715/2015 and FHC/L/CS/716/2015

*Orogun v. Federal Republic of Nigeria* (2018) 17 NWLR (Pt. 1648) 463 at 490

*Federal Republic of Nigeria v. Kingsley Eze* (2016) (CA/YL/68c/2015) NGCA 45

*Economic and Financial Crimes Commission v. Binance Holdings Ltd* (2024) (FHC/ABJ/CS/259)

*United States v. Ivanov, 175 F. Supp. 2d 367* (D. Conn. 2001)

*Federal Republic of Nigeria v. Fani-Kayode* (2010) 14 NWLR (Pt. 1214) 481 at 512

*Solomon Okedara v. Attorney General of the Federation* (2019) CA/L/174/18

*Dariye v. Federal Republic of Nigeria* (2015) 10 NWLR (Pt. 1467) 325 at 349

## ABSTRACT

This research focuses on the analysis of the effectiveness of cybercrime laws in Nigeria: Challenges and solutions. Despite the enactment of the Cybercrimes (Prohibition, Prevention, etc.), Act, 2015, Nigeria continues to struggle with enforcing its cybercrime laws effectively. This paper critically analyzes the effectiveness of Nigeria's cybercrime legal framework, identifies the systemic and operational challenges that hinder enforcement, and proposes viable solutions to improve the legal and institutional response to cyber threats. Drawing on scholarly sources, legal documents, and policy analysis, this study argues that while the legal framework is a significant step forward, its enforcement is undermined by weak institutional capacity, corruption, technological gaps, and low public awareness. The research concludes that the enactment of the Cybercrimes (Prohibition, Prevention, etc.), Act, 2015 marked a significant milestone in Nigeria's fight against digital crime. However, its effectiveness is hindered by structural, legal, and operational shortcomings. Low public awareness, poor enforcement capacity, outdated legal provisions, and weak institutional coordination continue to plague Nigeria's cybersecurity landscape. This study recommends that there should be periodic review and amendment of the Cybercrime Act to include modern cyber threats such as AI, cryptocurrency scams, and deep fakes. Sections that are vague, particularly those that threaten digital rights, should be redefined with clearer language; launch nationwide, multilingual cybercrime awareness programs via traditional media, social media, and grassroots outreach. Engage religious and community leaders to disseminate messages in rural areas; invest in the training of law enforcement agents, prosecutors, and judges on digital forensics, cyber law, and electronic evidence management. Establish cybercrime labs in collaboration with academia and the private sector and develop and adopt protocols for the admissibility of digital evidence in court, ensuring that data is collected and preserved in accordance with global best practices.

# CHAPTER ONE

# GENERAL INTRODUCTION

## 1.0 Introduction

Cyber-crime has emerged as one of the most disruptive and borderless threats faced by nations globally, affecting not only financial systems but also governance structures, critical infrastructure and individual liberties. In Nigeria, the increasing penetration of the internet, the rise of digital banking and the proliferation of social-media usage have simultaneously expanded the digital economy and increased vulnerability to online threats. These crimes range from phishing and cyber-stalking to ransomware attacks and business-email compromise (BEC), many of which now target banks, educational institutions and government platforms. The borderless nature of these crimes poses significant challenges to detection, prosecution and deterrence.

In acknowledgment of the seriousness of cyber threats, Nigeria enacted the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, the country's first comprehensive legislation to tackle offences such as identity-theft, system-hacking, child pornography, cyber-stalking and electronic fraud. The Act criminalised a wide array of cyber activities and laid out legal procedures for the investigation and prosecution of cyber offences.[1] Despite this progress, critics contend that the law has not kept pace with the dynamic and evolving nature of digital threats. For instance, cyber offences relating to blockchain technology and AI-generated content are not explicitly addressed, creating enforcement gaps.

The Nigerian legal system has struggled to apply the Cybercrimes Act effectively due to poor investigative capacity and inadequate infrastructure. *Federal Republic of Nigeria v. Justice*

[1] J Clough, '*Principles of Cybercrime,'* (Cambridge University Press, 2015), p. 47.

*Mohammed Yunusa* & 1 other,[2] cases which was publicly reported in TransparencIT in 2018, the defendant was charged with online fraud and identity-theft, but weak digital-evidence handling led to acquittal. Likewise, in *Nwankwoala v. Federal Republic of Nigeria*,[3] the Court of Appeal affirmed that the prosecution in a cyber-related or economic-crime case must establish all elements of the offence beyond a reasonable doubt, particularly the link between the accused and the fraudulent acts alleged. The court stressed that mere suspicion, digital traces, or uncorroborated electronic evidence are insufficient without credible, admissible proof directly tying the defendant to the commission of the crime. Ultimately, the decision reinforces the principle that criminal liability cannot be inferred from assumptions or technological associations alone only from properly proved and admissible evidence.

Cyber-crime cases are often transnational and technically complex, requiring specialised training and cross-border cooperation, which remain under-developed in Nigeria. Globally, countries are reforming and updating their cybersecurity laws to reflect emerging threats, data-sovereignty issues and digital-evidence protocols. Nigeria must do the same to remain relevant and effective in addressing cybersecurity challenges. Strengthening institutional synergy and digital-forensics capacity is vital for the sustainability of the legal framework.[4]

Accordingly, this study aims to critically analyse the scope and enforcement of Nigeria's cyber-crime laws, investigate institutional performance, assess public awareness and identify gaps that hinder legal effectiveness. It draws comparisons with international best practices and local realities, in order to formulate policy-driven solutions that are both relevant and actionable. Given the growing economic and social costs of cyber-crime, this research is timely and

---

[2] (2018) FHC/L/CS/ 714/2015, FHC/L/CS/715/2015 and FHC/L/CS/716/2015, https://v1.corruptioncases.ng/export/frn-vs-justice-mohammed-yunusa-former?utm_source=chatgpt.com

[3] (2018) 14 NWLR (Pt. 1639) 459 at 482

[4] L Ani, 'Cybersecurity and Digital Rights in Africa' (2020) *Journal of African Law,* 64 (2).

necessary. Cybersecurity issues require a hybrid of legal reforms, awareness campaigns and inter-agency collaboration.[5] Therefore, this study is positioned to contribute significantly to Nigeria's cybersecurity discourse and legal transformation by offering practical insights and recommendations.

### 1.1 Background of the Study

The exponential growth of Information and Communication Technology (ICT) has brought about unparalleled convenience and innovation across various sectors. However, it has also opened the flood-gates for sophisticated cyber-crime activities. In Nigeria, online-fraud schemes such as "Yahoo Yahoo", ATM-cloning, phishing and data-breaches have become pervasive, especially with the rise of mobile-money platforms. As early as 2010, the Economic and Financial Crimes Commission (EFCC) began warning about the growing threat posed by cyber-criminal syndicates operating both within and outside the country.[6]

The Cybercrimes Act of 2015 was a significant step in regulating digital activity and protecting citizens, corporations and critical infrastructure. It provided legal backing to prosecute cyber-stalking, fraud, cyber-terrorism and unlawful interception of communications. Nonetheless, application of this Act in real-world cases has revealed institutional and procedural limitations. For example, in *Orogun v. Federal Republic of Nigeria*,[7] the Court of Appeal emphasized that for economic-crime and cyber-related offences, the prosecution must present credible, admissible evidence directly linking the accused to the alleged fraudulent acts, and not rely on suspicion or assumptions. The court also reaffirmed that once the prosecution establishes a prima facie case,

---

[5]A Akinsola, *'*Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward Proc. of the International Conference on Computing and Advances in Information Technology (ICCAIT, 2023),' *Research gate Journal,* 21-23.

[6] Economic and Financial Crimes Commission (EFCC, 2010).

[7] *(*2018) 17 NWLR (Pt. 1648) 463 at 490.

the burden shifts to the defendant to offer a reasonable explanation, failing which the conviction will be sustained.[8]

A major issue in the Nigerian context is that law enforcement agencies lack specialised training in digital forensics, which impacts their ability to gather admissible evidence. Many officers are unfamiliar with metadata analysis, IP-tracing and blockchain investigations tools now essential in today's cyber-crime landscape. This lack of expertise reduces conviction rates and compromises investigations.[9]

Equally concerning is the limited public awareness of cybersecurity practices and legal protections. Consequently, digital literacy remains low particularly in rural areas and among older populations. Many Nigerians unknowingly fall victim to scams or, worse, engage in cyber-crime without understanding the legal implications. In *Federal Republic of Nigeria v Kingsley Eze*,[10] for instance, the defendant claimed ignorance of the law after being charged with impersonation via social media, reflecting this awareness gap.

Poor institutional coordination also affects enforcement of cyber-crime legislation. Agencies such as the EFCC, the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC) often lack harmonised operational frameworks, which leads to duplication of roles and jurisdictional disputes. In an internal review of Nigerian Communications Commission and Anonymous ISP Case of 2019, involving illegal Internet-service operations, failure by law-enforcement to act promptly was attributed to ambiguity over primary agency authority.[11]

---

[8] E Ani, 'Cybersecurity and Digital Rights in Africa' 2020 *Journal of African Law*, 64(2), 112.
[9] D Dasgupta, *Introduction to Cybersecurity: A Multidisciplinary Challenge* (Springer 2024) 1-16,
[10] *Federal Republic of Nigeria vs Kingsley Eze* (2016) (CA/YL/68c/2015) NGCA 45; P. C. Agba, 'International Communication Principles, Concepts and Issues". In C. S. Okunna (Ed.), *Techniques of Mass Communication: A Multi-Dimensional Approach* (Enugu: New Generation Books, 2003), 9.
[11] F Ibikunle and O Eweniyi, 'Cybersecurity in Nigeria: A National Concern,' International Journal of Computer Applications, (2013), 67(20); NIBSS (2024). Annual Fraud Report. Lagos, and Federal Republic of Nigeria v

The cumulative effect of these challenges is that many cyber-crime cases are either not prosecuted or struck out due to procedural lapses. This trend contributes to public scepticism about the efficacy of Nigeria's cyber-crime law and emboldens cyber-criminals. This study seeks to explore how these systemic issues can be resolved through institutional reform and legal amendment. Understanding the legal, technical and social dimensions of cyber-crime is essential for developing a comprehensive and proactive strategy. This research fills a gap in legal literature by analysing the effectiveness of cyber-crime laws in Nigeria: challenges and solutions, while offering actionable recommendations.

**1.2 Statement of the Problem**

Cyber-crime in Nigeria has evolved into a growing national and international concern. According to the International Criminal Police Organization (INTERPOL) of 2025, Africa Cyber-threat Assessment Report, Nigeria ranked third in Africa for ransomware threat detections in 2024, with 3,459 recorded incidents.[12] Beyond ransomware, other widespread threats include business-email compromise, extortion and online scams. The Nigeria Police Force's National Cybercrime Centre (NPF-NCCC) recorded major successes in 2024, dismantling over 5,049 malicious domains, arresting more than 751 individuals, and recovering N8.821 billion, 115,237.91 USDT and USD 84,000 in assets. [13]

Despite these victories, Nigeria's financial sector continues to suffer large losses, with many billions of naira being siphoned annually. For instance, Nigerian businesses faced an average of

---

Kingsley Eze (CA/YL/68c/2015) NGCA 45 (5 May 2016), Nigerian Communications Commission v Anonymous ISP Case (2019).

[12] NTERPOL Africa Cyberthreat Assessment Report 2025, 4th edition, 25COM009248%20-%20Cybercrime _Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf, 2025.

[13] Nigeria Police Force – National Cybercrime Centre. **2024**. *Title of Press Release or Report.* Accessed [date]. https://example-source, assessed November 2025

4,388 cyber-attacks per week in the first quarter of 2025, a 47 % increase on previous figures.[14] A critical problem is the weak enforcement of existing cyber-laws. In *Solomon Okedara v. Attorney General of the Federation Court of Appeal*, In *Julius v. Federal Republic of Nigeria* ,[15] the Court of Appeal affirmed a conviction under Section 13 of the Cybercrimes Act for "computer-related forgery," holding that Julius had published inauthentic information on his Facebook platform that could mislead the public. The court reduced his sentence to 3 years' imprisonment or a ₦7,000,000 fine**,** noting that the prosecution failed to prove several of the other counts beyond reasonable doubt.

Consequently, there are legal ambiguities within the Cybercrimes Act itself. Provisions regarding data privacy, cryptocurrency fraud and cross-border digital surveillance remain unclear. In *Dr. Imoro Kubor v. Seriake Henry Dickson* is the leading Nigerian authority on the admissibility of computer-generated evidence under Section 84 of the evidence Act 2011.[16] The Supreme Court held that electronic materials (such as online printouts, computer documents, and digital records) are inadmissible unless the party tendering them strictly complies with Section 84 by providing proper certification and demonstrating the reliability of the computer system used. Public ignorance about cyber-laws and digital safety protocols is another challenge. Outlined below are the key problems associated with this study:

a. **Weak enforcement capacity**: Law-enforcement agencies often lack the technical skills, tools and training needed to investigate and prosecute cyber-crimes effectively.

[14] Balogun, Folake. "Nigerian Organisations Recorded 4,388 Attacks per Week in Q1 Check Point" 17 Apr. 2025.*BusinessDay*,.
[15] (2019), CA/L/174/1.
[16] (2013) 4 NWLR (Pt. 1345) 534.

b. **Legal ambiguities and gaps**: The Cybercrimes Act of 2015 does not adequately address emerging digital threats such as cryptocurrency fraud, AI-driven scams and blockchain-related crimes.

c. **Low public awareness**: A significant portion of the Nigerian population lacks awareness of cyber-crime laws and basic cybersecurity practices, leading to increased victimisation and unintentional participation in cyber-offences.

d. **Inadequate digital infrastructure**: Poor access to reliable forensic tools, outdated IT systems and lack of nationwide cybersecurity infrastructure hinder proactive crime detection and response.

e. **Poor inter-agency coordination**: Agencies like the EFCC, NCC and NITDA often work in silos, leading to duplication of efforts, jurisdictional confusion and ineffective case-management.

f. **Slow judicial processes**: Delays in prosecuting cyber-crime cases due to back-logs, lack of specialised cyber-crime courts and limited judicial expertise reduce the deterrent effect of the law.

g. **Increasing sophistication of cyber-criminals**: Cyber-criminals in Nigeria are rapidly adopting more complex and technologically advanced methods, often outpacing the capability of current legal and enforcement frameworks.[17]

Consequently, insufficient collaboration between enforcement and regulatory agencies also impedes progress. For example, in a joint operation under *Economic and Financial Crimes Commission v. Binance Holdings Ltd*,[18] the Federal High Court in Abuja granted the EFCC's ex-parte application directing Binance to hand over comprehensive data on all Nigerians trading on

[17] S W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law'" *Murdoch University Electronic Journal of Law* (2001) 8(2) 3–12.
[18] (2024), FHC/ABJ/CS/259.

its platform. This order underscores the court's willingness to compel global crypto platforms to cooperate in investigations into alleged money-laundering and terror financing. Without urgent reforms in training, legal provisions and public sensitisation, Nigeria's cyberspace will remain exposed to persistent criminal exploitation. This study therefore seeks to interrogate these issues and propose actionable solutions for enhancing the country's cybersecurity governance.

### 1.3 Research Questions

This research will answer the following questions'.

1. What is the scope and adequacy of existing cybercrime laws in Nigeria, particularly the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015?
2. What is the level of public awareness regarding cybercrime laws and cybersecurity practices in Nigeria?
3. What institutional and enforcement mechanisms are in place for combating cybercrime in Nigeria, and how effective are they?
4. What are the major legal challenges affecting the enforcement of cybercrime laws in Nigeria and possible solutions?

### 1.4 Aim and Objectives of the Study

The aim of this study is to critically analyze the effectiveness of cybercrime laws in Nigeria, and the challenges hindering their implementation,

1. To assess the scope and adequacy of existing cybercrime laws in Nigeria, particularly the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
2. To analyze the level of public awareness regarding cybercrime laws and cybersecurity practices in Nigeria.

3. To examine the institutional and enforcement mechanisms in place for combating cybercrime in Nigeria.
4. To identify the major legal challenges affecting the enforcement of cybercrime laws in Nigeria and possible solutions.

1.5 Research Methodology

This long essay will adopt the doctrinal research method. It will rely on primary sources including case law, constitutional provisions, and enacted legislation to guide the analysis. In addition, data will be sourced from secondary materials**,** including relevant statutes such as the *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*, judicial decisions, scholarly articles, government policy documents, and reports from enforcement agencies like the EFCC and NCC. Content analysis will be employed to evaluate the strengths, weaknesses, and enforcement gaps of current cybercrime legislation.[19]

1.6 Scope of the Study

The scope of this study is limited to analyzing the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and other related laws as they apply within Nigeria. It focuses on the effectiveness of the legal framework, challenges facing its enforcement, the level of public awareness, and the institutional capacity of enforcement bodies. The study does not cover the technical dimensions of cybersecurity infrastructure in detail but instead emphasizes legal, policy, and institutional responses. Geographically, the study focuses on Nigeria as a case study, with examples drawn from relevant legal and policy documents and selected judicial decisions within Nigerian courts.

1.7 Significance of the Study

This study is significant as it contributes to the expanding discourse on cybercrime regulation, cybersecurity governance, and digital justice in Nigeria. By identifying the practical challenges

[19] NIBSS (2024). Annual Fraud Report. Lagos.

confronting law enforcement agencies, regulatory institutions, and the judiciary, the study provides critical insights that can inform legislative reforms, institutional capacity-building, and improved inter-agency coordination. It also assesses the practical enforcement of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 offering strategic recommendations for strengthening Nigeria's cybercrime response mechanisms in line with international best practices. This study holds value for a broad range of stakeholders:

i. Legal practitioners and policymakers will benefit from a clearer understanding of existing legal gaps, implementation challenges, and the need for reforms within the cybercrime legal framework.

ii. Security agencies and regulatory bodies such as the EFCC, NCC, and NDPC will gain from the analysis of enforcement obstacles and the recommendations for improved synergy, digital forensics, and prosecution capabilities.

iii. Technology firms, financial institutions, and service providers will be better informed about compliance requirements under Nigeria's cybercrime laws, as well as the legal risks of weak cybersecurity systems.

iv. The Nigerian public and digital users will become more aware of their rights, responsibilities, and the protections offered under current cyber laws, promoting safer digital practices.

v. Researchers and academic institutions will find this study useful for further exploration into cyber law, digital security, and legal-institutional responses to technological threats in Nigeria and similar jurisdictions.

Ultimately, this study bridges the gap between legal theory and practical enforcement by offering policy-relevant recommendations aimed at enhancing the effectiveness of Nigeria's cybercrime laws and safeguarding the nation's digital ecosystem.

## 1.9 Limitation of the Study

This study is limited by inadequate access to up-to-date and comprehensive data on cybercrime incidents and prosecutions in Nigeria, which restricts the depth of empirical analysis. Additionally, the research focuses primarily on federal legislation, thereby excluding state-level initiatives and international cooperation frameworks that could further influence the effectiveness of cybercrime laws.

## 1.9 Chapter Analysis

This chapter one contains the background to the study, statement of the problem, objectives of the study, research questions, scope and limitations, significance, and methodology. It provides an overview of cybercrime in Nigeria and introduces the legal framework governing cyber activities, thereby setting the foundation for subsequent chapters. This chapter two discusses the conceptual clarification of key terms such as cybercrime, cybersecurity, and digital evidence. It review theoretical and historical foundations and literature review. This chapter three provides a detailed analysis of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, and other related statutes such as the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Evidence Act, and international conventions ratified by Nigeria. It evaluates the adequacy, strengths, and weaknesses of these laws in addressing cybercrime. This chapter four critically examines the institutional, technical, and procedural challenges that hinder the effective enforcement of cybercrime laws in Nigeria. Issues such as inadequate capacity of law enforcement agencies, jurisdictional conflicts, poor inter-agency coordination, and low public awareness are discussed with relevant case studies and practical examples. This chapter five presents a concise summary of the entire study, outlines the key findings, and offers recommendations aimed at strengthening the effectiveness of cybercrime laws in Nigeria. It

suggests legal, institutional, and policy reforms necessary for combating cybercrime and ensuring a secure digital environment.

# CHAPTER TWO

# CONCEPTUAL CLARIFICATION, THEORETICAL AND HISTORICAL FOUNDATION AND LITERATURE REVIEW

## 2.0 Introduction

This section reviews cybercrime as one of the most pressing challenges of the digital age, reshaping how nations, organisations, and individuals protect their information. With rapid technological advancement and increasing reliance on online systems, opportunities for exploitation have grown just as quickly. Also this section discusses cybersecurity which has become a central focus for governments and businesses striving to safeguard their digital environments. These developments highlight the urgency of strengthening resilience against evolving threats in cyberspace. Hence;

- Cybercrime
- Cybersecurity

## 2.1 Conceptual Clarification

### 2.1.1 Cybercrime

The term *cybercrime* broadly refers to criminal activities that are either committed through the use of computers, digital networks, or electronic communication systems, or are targeted at such systems. Scholars generally describe it as the unlawful act in which technology serves as either the object or the tool of the offence.[20] Cybercrime represents a convergence of technology and crime, where offenders exploit the anonymity, speed, and global connectivity of the internet to perpetrate unlawful acts.[21] According to Furnell and Warren, cybercrime encompasses a wide

[20] D S Wall, '*Cybercrime: The Transformation of Crime in the Information Age,'* (Cambridge, United Kingdom: Polity Press, 2007); S W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law,' (2001) *Murdoch University Electronic Journal of Law* 8(2) 3–12.
[21] P 'Grabosky, *Cybercrime: Problems of Classification and Conceptualization,'* (Cham, Springer 2016).

spectrum of offences, including identity theft, internet fraud, phishing, cyberstalking, hacking, online impersonation, and other forms of computer-enabled misconduct.[22] These crimes are often motivated by financial gain, political objectives, or personal vendettas, and may be directed against individuals, corporations, or government institutions. The consequences are far-reaching, frequently resulting in financial loss, data breaches, privacy violations, and reputational damage.

In the Nigerian context, the *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015* serves as the principal legislative framework for regulating and penalizing cyber-related offences. The Act defines a wide range of computer-based crimes and provides for mechanisms of investigation, prosecution, and international cooperation. It further imposes obligations on financial institutions and service providers to safeguard digital infrastructure and report suspicious cyber incidents.[23] By establishing these provisions, the Act aligns Nigeria's regulatory environment with international best practices and reinforces the government's commitment to promoting a secure and trustworthy cyberspace. Ultimately, the legislation serves as both a deterrent and a corrective tool for addressing the growing threat of cybercrime within and beyond Nigeria's borders.

According to Olayemi, cybercrime in Nigeria has evolved significantly over the past two decades from the relatively simple email scams of the early 2000s, popularly known as *"Yahoo Yahoo"*, to more sophisticated and transnational digital offences.[24] Similarly, scams were largely social engineering schemes relying on deception and psychological manipulation to defraud

---

[22] S Furnell and M Warren, 'Computer Security, Cybercrime, and Cybersecurity: A Comparative Introduction' (2019) *Computers and Security* 87(1), 101589, and The *Cybercrimes (Prohibition, Prevention, etc.) Act,* 2015.

[23]G S Osho and J Olayemi, 'Cybercrime and Cybersecurity in Nigeria: The Role of Legislation,' (2018) *African Journal of Criminology and Justice Studies* 11(1) 89–104.; O.J. Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria' (2014) I*nternational Journal of Sociology and Anthropology* 6(3) 116–125.

[24] Ibid.

unsuspecting victims, both locally and internationally.[25] However, with technological advancement and increased internet penetration, Nigerian cybercriminals have expanded their operations into complex domains such as cryptocurrency fraud, ransom-ware attacks, online identity theft, and corporate data breaches. These emerging trends demonstrate the dynamic nature of cybercrime and its capacity to adapt to new digital tools and global financial systems. Consequently, cybercrime in Nigeria has moved beyond individual opportunism to organized, transnational criminal networks that exploit loopholes in cybersecurity and digital governance structures.

*Cybercrime* refers to any unlawful activity that employs computers, mobile devices, or digital networks as either the main instrument or the object of the offence. It is a product of the intersection between technological innovation and criminal intent, representing a modern extension of traditional crime into the digital domain. Nigerian scholars such as Olayemi and Osho and Olayemi, describe cybercrime as any illegal act conducted through electronic means, including fraud, identity theft, and unauthorized access to data or systems.[26] It covers a wide range of offences such as hacking, phishing, cyberstalking, data breaches, online impersonation, and financial scams. Unlike conventional crimes, cybercrime is borderless and asynchronous it can be perpetrated from any location and often without the physical presence of the offender or direct contact with the victim.

One of the distinguishing features of cybercrime is its heavy reliance on digital infrastructures and the exploitation of technological vulnerabilities. Cybercriminals often manipulate

---

[25] O Tade and O Adeniyi, "Yahoo Boys" and Criminal Entrepreneurship in Nigeria' (2019) *International Journal of Cyber Criminology* 13(1) 61–79.

[26] O J Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria' (2014) I*nternational Journal of Sociology and Anthropology* 6(3) 116–125; G.S. Osho & J. Olayemi, 'Cybercrime and Cybersecurity in Nigeria: The Role of Legislation' (2018) *African Journal of Criminology and Justice Studies* 11(1) 89–104..

weaknesses in operating systems, social media platforms, and human behaviour to gain unauthorized access to sensitive data, disrupt networks, or steal financial information. For instance, the International Telecommunication Union of 2020 categorizes cybercrime into offences such as illegal access, data interference, and system interference, misuse of devices, and computer-related fraud or forgery. Within the Nigerian context, the *Cybercrimes (Prohibition, Prevention, etc.), Act, 2015* adopts similar classifications, reflecting the country's effort to align domestic laws with international cyber norms.[27]

Moreover, the Nigerian cybercrime landscape exhibits unique socio-economic and cultural dimensions. The phenomenon of "Yahoo Yahoo" or internet scamming illustrates how cybercrime has evolved into a form of organised digital enterprise among youth populations, driven by unemployment, peer influence, and moral ambivalence.[28] Consequently, cybercrime in Nigeria is not only a technological issue but also a social, legal, and developmental concern requiring a multifaceted response from government agencies, educational institutions, and the private sector. The motive behind these crimes may be financial gain, espionage, political activism, or even revenge, depending on the type and intent of the perpetrator.

Globally, *cybercrime* has emerged as one of the most pervasive and fastest-growing forms of criminal activity, posing significant threats to individuals, corporations, and national governments. It transcends geographical and jurisdictional boundaries, operating within a borderless digital environment that complicates detection, regulation, and prosecution. According to the International Criminal Police Organization (INTERPOL) of 2023 and *the* World Economic Forum of 2024*,* cybercrime now ranks among the top global security risks,

---

[27] I E Nwaobilo and U C Umearokwu, 'Cybersecurity as a National Concern: Implications for Nigeria's Digital Economy' *Nigerian",'* International Telecommunication Union (ITU, 2020), (2024) *Journal of Information Security Studies* 3(1) 21–39.

[28] Ibid (n23).

with economic losses estimated in trillions of dollars annually.[29] Financial institutions, healthcare providers, and government agencies are prime targets due to the vast amounts of sensitive data and critical infrastructure they manage. Cybercriminals exploit these vulnerabilities for monetary gain, espionage, and strategic disruption.[30]

In Nigeria, the accelerated digitalisation of the economy and society has coincided with a notable increase in cybercrime activities. The rapid expansion of internet access, widespread use of smartphones, and the growth of e-commerce and digital payment platforms have created new opportunities and targets for cybercriminals. While this digital transformation has enhanced efficiency, convenience, and financial inclusion, it has not always been matched with adequate cybersecurity awareness, technological safeguards, or robust legal enforcement, leaving both individuals and institutions exposed.[31]

Socio-economic factors play a significant role in driving cybercrime. Poverty, youth unemployment, and limited economic opportunities have been identified as key motivators, particularly among university students and young adults. It is clear that economic challenges, digital access disparities, and peer or community influence were significant drivers of involvement in digital fraud. These findings mirror broader national trends, where socio-economic pressures intersect with technological opportunities to fuel cybercrime.[32]

These cases illustrate that cybercrime in Nigeria is multifaceted, ranging from individual opportunistic fraud to organized, technologically sophisticated operations. They also demonstrate how the legal system, through the EFCC and the Cybercrimes Act, attempts to deter and punish offenders while addressing socio-economic and technological drivers. Consequently, cyber-

[29] *International Criminal Police Organization (*INTERPOL, 2023) and the (2024) *World Economic Forum*
[30] Ibid (n28).
[31] Ibid (n26).
[32] Ibid (n26).

crime in Nigeria manifests in several forms, ranging from email scams and identity theft to more sophisticated attacks such as ransom-ware, online banking fraud, social engineering and Business Email Compromise (BEC). For example:

The legal and institutional framework for combating cybercrime in Nigeria is anchored primarily on the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which provides the foundational legislative instrument for defining, preventing, and punishing cyber-related offences. The Act encompasses a broad range of crimes including computer fraud, identity theft, phishing, cyberstalking, and electronic fraud, while also outlining the responsibilities of service providers and mechanisms for international cooperation.[33]

Complementing this legal framework are key institutional actors tasked with enforcement and mitigation of cybercrime. The Economic and Financial Crimes Commission (EFCC) leads in investigating and prosecuting cyber-enabled financial crimes. The Nigeria Computer Emergency Response Team (ngCERT) is responsible for monitoring and responding to cyber threats, while the Nigeria Police Force Cybercrime Unit undertakes detection, intelligence gathering, and operational enforcement.[34] Collectively, these institutions represent the operational backbone of Nigeria's cybersecurity enforcement landscape.

However, despite these structures, enforcement remains inconsistent, and challenges persist. Consequently, the phenomenon of "Yahoo plus", the use of spiritual or occult practices to enhance online fraud as a demonstration of the limitations of existing legal frameworks and enforcement mechanisms. In the landmark case of *Olagunju v. Federal Republic of Nigeria*, the court in addressed the scope of the EFCC's authority to investigate and prosecute financial and

[33] Cybercrimes Act, 2015; I.E. Nwaobilo and U.C. Umearokwu, 'Cybersecurity as a National Concern: Implications for Nigeria's Digital Economy' *Nigerian"* (2024) *Journal of Information Security Studies* 3(1) 21–39.
[34] Ibid (n26).

economic crimes under its establishing statute.[35] It affirmed that the EFCC possesses independent prosecutorial powers and may initiate proceedings without requiring prior authorization from the Attorney General. The case reinforced the judicial trend of upholding the EFCC's autonomy while clarifying the constitutional limits of its enforcement powers.

Further critiques point to the outdated and reactive nature of Nigeria's cybercrime law. However, the legislation requires significant modernization to keep pace with evolving cyber threats, including ransomware, cryptocurrency fraud, and corporate espionage.[36] Recommendations include the establishment of specialised cybercrime courts, continuous training of judges in digital forensics, and the introduction of updated punitive measures aligned with contemporary cyber threats. For instance, the *Federal High Court in Olagunju v. Federal Republic of Nigeria* reaffirmed the EFCC's authority to investigate and prosecute financial crimes without requiring prior authorization from the Attorney General.[37] The decision strengthened the Commission's institutional autonomy while clarifying the constitutional boundaries of its prosecutorial powers.[38] While Nigeria has made considerable strides in establishing both legal and institutional mechanisms to combat cybercrime, enforcement challenges, socio-cultural peculiarities, and technological sophistication of offenders highlight the need for continuous legislative updates, capacity building, and multi-agency collaboration. Strengthening these dimensions is critical to safeguarding Nigeria's digital economy and aligning national cybercrime responses with global best practices.

### 2.1.2 Concept of Cybersecurity

[35] (2018) 10 NWLR (Pt 1627) 272.
[36] L Ani, 'Cybercrime and National Security: The Role of the Penal and Procedural Law' in *Law and Security in Nigeria* (2015) *Journal of Art* 197–231
[37] (2018) 10 NWLR (Pt 1627) 272
[38] Ibid (n1).

Cybersecurity has been widely recognized as a cornerstone of the modern digital ecosystem, encompassing a comprehensive framework of technological, legal, and organizational safeguards designed to protect digital systems, networks, and data from unauthorized access, misuse, alteration, or destruction. Dasgupta and Gupta & Agrawal established that cybersecurity serves as the collective mechanism for ensuring the confidentiality, integrity, and availability (CIA) of digital information three interdependent principles essential to maintaining the reliability and security of data. It is clear that effective communication and security infrastructures are indispensable to sustaining public confidence and stability in modern information societies. Consequently, cybersecurity transcends the technical domain to incorporate behavioral, regulatory, and institutional elements that collectively ensure the secure and responsible use of cyberspace.[39]

According to the International Telecommunication Union (ITU), cybersecurity refers to the assemblage of tools, policies, security concepts, and best practices aimed at safeguarding the cyber environment and user assets. This definition, as Ladan emphasized, demonstrates that cybersecurity operates not merely as a technological concern but as a multi-sectoral governance issue that demands coordination between law, policy, and digital infrastructure.[40] Similarly argued that a holistic cybersecurity framework is fundamental for preventing malicious acts such as malware distribution, phishing attacks, ransomware infiltration, and identity theft. In this

[39] D Dasgupta, 'Computational Intelligence in Cyber Security', in *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (CIHSPS 2006) 2–3; S. Gupta and B. Agrawal, *Cyber Laws: Law Relating to Information Technology, Hacking, Intellectual Property Rights, Trade Marks, E-Commerce, Computers, Computer Software, Internet and Cybercrimes* (Allahabad, India: Premier Publishing Co. 2009) 221; P. C. Agba,. "International Communication Principles, Concepts and Issues", In C. S. Okunna (Ed.), *Techniques of Mass Communication: A Multi-Dimensional Approach*. (Enugu: New Generation Books 2003), 13.

[40] M T Ladan, *Cyberlaw and Policy on Information and Communications Technology in Nigeria* (Zaria: Ahmadu Bello University Press 2015) 104.

regard, cybersecurity functions as both a preventive and responsive mechanism**,** strengthening public trust, digital privacy, and the resilience of critical information systems.

Cybersecurity manifests through several interrelated domains. Network security appears to be concentrates on protecting communication channels from intrusion using encryption, firewalls, and intrusion detection systems. Information security (InfoSec) ensures that data remains authentic, confidential, and accessible only to authorized users, while application security**,** helps to mitigates vulnerabilities in software applications, preventing exploits such as cross-site scripting or Structured Query Language (SQL) injection. Operational security (OpSec) manages the human and procedural dimensions of data handling to minimize risks associated with insider threats.[41] Furthermore, endpoint security defends devices such as laptops and mobile phones frequent entry points for cyberattacks while cloud security**,** describes leverages encryption and multifactor authentication to secure virtual storage environments. Finally, critical infrastructure security protects essential national systems such as telecommunications, banking, and energy networks, which have been designated as National Critical Information Infrastructure (NCII) under th*e* Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.[42]

There is a strong argument that cybersecurity is a vital determinant of national security, economic development, and societal stability. In Nigeria's rapidly evolving digital economy, cyber threats ranging from online fraud and identity theft to cyberstalking have become increasingly sophisticated.[43] Therefore, enhancing cybersecurity is not merely a technical

---

[41]Y A Makeri, 'Cyber Security Issues in Nigeria and Challenges,' (2017) *International Journal of Advanced Research in Computer Science and Software Engineering,* 7(4), 315–321.

[42] Ibid.; I J Fehintola, *An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria* (Crescent University, Abeokuta, 2023) 42; O J Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria' (2014) I*nternational Journal of Sociology and Anthropology* 6(3) 116–125.

[43] Ibid (n46).

necessity but a national imperative for safeguarding citizens' digital rights and preserving the integrity of governance systems.[44]

To address these emerging risks, the Nigerian government enacted the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which serves as the primary legal instrument for combating cyber threats. The Act criminalizes various offenses including hacking, cyberstalking, cyberterrorism, and identity theft and empowers the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), and the Office of the National Security Adviser (ONSA) to investigate and prosecute such crimes.[45] Judicial precedents across Nigeria have demonstrated the judiciary's commitment to enforcing this framework. For instance, in *Federal Republic of Nigeria v. Osasuyi Aisosa*, the court convicted the defendant for using fraudulent emails to obtain funds, thereby illustrating how the judiciary enforces deterrence against cyber-enabled fraud. Likewise, in *Federal Republic of Nigeria* v. Kingsley Nwosu,[46] the Federal High Court applied Section 22 of the Act to convict the defendant for identity theft and impersonation, reaffirming the legal applicability of digital evidence. In *Federal Republic of Nigeria v. Bashir Umar*, the court upheld the admissibility of forensic electronic data, thereby establishing judicial recognition of digital forensics in Nigerian criminal jurisprudence.[47]

Beyond punitive enforcement, the Cybercrimes Act, 2015, emphasizes data protection and retention as a foundational aspect of cybersecurity governance. Sections 38 to 40 of the Act impose obligations on telecommunications service providers and Internet Service Providers (ISPs) to retain user traffic and subscriber information for a minimum of two years to facilitate law enforcement investigations. This statutory obligation enhances traceability and

[44] F Ibikunle, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution,' (2013) *Department of Electrical & Information Engineering, Covenant University Nigeria* 1(1) 1.; (n51).
[45] Federal Republic of Nigeria. *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.* Abuja: Federal Government Printer.
[46] (2021), FHC/EN/CR/132.
[47] (2020), FHC/ABJ/CR/279

accountability in digital communications.[48] Similarly, under Section 37**,** financial institutions are required to implement comprehensive cybersecurity frameworks to prevent and report suspicious cyber-related activities. The judicial position in *Federal Republic of Nigeria v. Ayoola Samson*, reinforced institutional responsibility, as the court held a financial systems operator liable for failing to prevent unauthorized access to customers' accounts, thereby asserting the duty of care owed by institutions under the Act.[49]

The Act further promotes international cooperation through Section 44**,** which provides for mutual legal assistance (MLA) and cross-border evidence exchange. This provision aligns Nigeria's legal framework with international cybersecurity norms and enhances collaboration with entities such as INTERPOL, ECOWAS, and the African Union. The decision in *Socio-Economic Rights and Accountability Project (SERAP) v. Federal Republic of Nigeria*, before the ECOWAS Court of Justice underscored the necessity of harmonizing Nigeria's cyber legislation, particularly Section 24, with international human rights standards relating to privacy and freedom of expression.[50] This judgment demonstrated the regional commitment to ensuring that cybersecurity measures do not infringe upon fundamental rights.

Furthermore, the Act enforces regulatory compliance across all sectors of the economy. Hence, telecommunication and Internet service providers play a crucial role in national cyber defense and must cooperate fully with investigative authorities. Corporate organizations bear legal responsibility for adopting security frameworks commensurate with the sensitivity of their data

---

[48] O Olanipekun, 'Cybercrimes in the Banking Sector: Facing the New Wave of Criminals Legally,' (2015) *Business Intelligence Journal* 3(1) 98-99.

[49] Ibid, and others, such as, the *Federal Republic of Nigeria* vs. *Kingsley Nwosu* (2021), FHC/EN/CR/132, *Federal Republic of Nigeria vs. Bashir Umar* (2020), FHC/ABJ/CR/279, *Federal Republic of Nigeria vs. Emeka Okechukwu*, 2021), *Federal Republic of Nigeria vs. Ayoola Samson* (2022), FHC/IB/CR/42.

[50] Sahara Reporters, *ECOWAS Court Declares 'Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful* 2023, March 22) *and Socio-Economic Rights and Accountability Project (SERAP) vs. Federal Republic of Nigeria* (2023), ECW/CCJ/APP/17/19*,* M T Ladan, '*Cyberlaw and Policy on Information and Communications Technology in Nigeria,'* (Ahmadu Bello University Press, 2015) 104.

operations. Similarly, non-compliance with cybersecurity regulations may attract both administrative and criminal sanctions, thereby fostering a culture of digital accountability and responsible data management within Nigeria's socio-economic landscape.[51]

Penalties under the Cybercrimes Act vary according to the gravity of the offense. For instance, cyberstalking**,** under Section 24**,** attracts imprisonment of up to ten years or a fine of ₦25 million, or both; cyberterrorism, under Section 18**,** may result in life imprisonment; and identity theft**,** under Section 22**,** carries a penalty of up to three years imprisonment or a ₦7 million fine. These provisions have been judicially enforced in *Federal Republic of Nigeria v. Ndukwe & Anor*,[52] Port Harcourt and *Federal Republic of Nigeria v. Oduwale Olumide*, Akure,[53] where the courts convicted defendants for phishing and unauthorized access to computer systems, respectively. Such judicial interventions, revealed the Nigerian judiciary's evolving approach to digital justice and its responsiveness to global trends in cyber law enforcement.[54]

Consequently, cybersecurity in Nigeria represents a multi-dimensional construct encompassing technical, legal, and institutional measures designed to protect the integrity of the nation's digital environment. The success of Nigeria's cybersecurity framework depends on periodic legislative review**,** capacity building**,** and enhanced inter-agency coordination**.** As the cyber landscape continues to evolve, a robust and adaptive cybersecurity system remains vital not only for protecting national infrastructure but also for sustaining economic growth, digital trust, and the fundamental rights of citizens in the global information society.[55]

## 2.2 Theoretical and Historical Foundation

---

[51] S Oho, *A Critical Analysis of the Cybercrime Law in Nigeria* (Baze University, Abuja, 2017).; E. Ogana, *An Analysis of Legal Framework on Combating Cybercrime in Nigeria* (Master's Dissertation, Ahmadu Bello University, Zaria, 2017) 17–214.
[52] (2018), FHC/PH/CR/110/2018, Port Harcourt.
[53] (2021), FHC/AK/CR/56/2021, Akure.
[54] Ibid (n50).
[55] Ibid.

The development of cybercrime legislation in Nigeria can be examined through two key theoretical lenses: the legal-institutional theory and the routine activity theory. Together, these frameworks provide both a structural and sociological understanding of how Nigeria's cybercrime laws have evolved and how they operate within the country's socio-economic and technological contexts.

**Legal-Institutional Perspective**

From a legal-institutional standpoint, Nigeria's cybercrime framework, most notably the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 was a reactive legislative response to mounting internal and external pressures rather than a proactive policy initiative. The increasing prevalence of financial crimes, identity theft, and internet fraud,[56] often linked to Nigerian actors, significantly tarnished the country's international image. The government faced diplomatic criticism for its perceived inaction in curbing cyber fraud, including high-profile cases of transnational scams and email fraud. This global reputational damage created a sense of urgency among policymakers, leading to the formulation of a comprehensive cybercrime law aimed at criminalizing digital offenses, reinforcing enforcement mechanisms, and signaling Nigeria's commitment to international cybersecurity standards.[57]

Kolawole's argument is crucial to this study because it highlights the reactive and image-driven genesis of Nigeria's cybercrime legislation. The Act emerged more out of necessity than foresight, filling existing legal voids only after significant socio-economic and diplomatic harm had occurred. Consequently, while the Act succeeded in consolidating disparate provisions and introducing legal deterrents, it initially lacked provisions for emerging threats such as cryptocurrency-related fraud, deepfakes, and AI-enabled phishing. This reactive posture

[56] A Kolawole, 'Cybercrime Legislation in Nigeria: Effectiveness and Gaps,' (2022) *ResearchGate* 1–6.
[57] Ibid.

underscores an enduring institutional weakness legislation that struggles to anticipate and adapt to rapidly evolving digital risks thus emphasizing the need for continuous policy reform and proactive governance.

Nigeria's cybercrime legislation within a broader international legal alignment framework. He argues that the 2015 Act was strategically harmonized with global and regional legal instruments, including the Budapest Convention on Cybercrime, the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), and various United Nations guidelines on digital crime prevention.[58] This alignment was not only instrumental for facilitating cross-border cooperation in cyber investigations, extraditions, and data sharing but also aimed at restoring investor confidence in Nigeria's financial and ICT sectors, which had been undermined by escalating cyberattacks.

In the context of this study, the legal-institutional evolution of Nigeria's cybercrime framework is instructive. It demonstrates that while the Cybercrimes Act 2015 represented a landmark policy intervention, its externally influenced design and reactive orientation limit its adaptability to local realities and technological advancements. Therefore, a holistic evaluation of its effectiveness requires both a legal assessment and an institutional critique questioning whether the law supports proactive digital governance or remains constrained by its reactionary origins. This theoretical grounding informs the study's focus on identifying enforcement gaps, assessing institutional capacity, and recommending adaptive reforms for a more resilient cybercrime control regime in Nigeria.[59]

**Routine Activity Theory**

[58] Ibid (n50).
[59] Ibid (n79)

The Routine Activity Theory (RAT), developed by Cohen and Felson, who provides a complementary sociological framework for understanding the prevalence of cybercrime in Nigeria. The theory posits that a crime occurs when three conditions converge: (1) a motivated offender, (2) a suitable target, and (3) the absence of a capable guardian. Applied to the digital sphere, these elements translate into tech-savvy but economically marginalized individuals as motivated offenders, unsecured systems or unsuspecting users as suitable targets, and weak cybersecurity infrastructure or ineffective law enforcement as the absence of capable guardians.

Nigeria's socio-economic environment marked by high youth unemployment,[60] expanding internet access, and poor digital literacy creates a conducive atmosphere for cybercriminal activities. Many young Nigerians, equipped with technological skills but lacking economic opportunities, are easily drawn into online scams, phishing, and other illicit digital practices. Meanwhile, underfunded law enforcement agencies, outdated investigative tools, and low cybersecurity awareness have left many institutions and individuals vulnerable, resulting in a fertile ecosystem for cybercrime. From a policy standpoint, the Routine Activity Theory underscores the need to strengthen guardianship mechanisms rather than relying solely on punitive approaches. Enhancing law enforcement capacity, improving public digital literacy, and deploying robust cybersecurity infrastructure such as firewalls, authentication protocols, and digital forensics labs are critical preventive measures. Moreover, addressing the root socio-economic drivers of cybercrime, including unemployment and poverty, is equally vital to reducing offender motivation.

This study, the Routine Activity Theory provides a valuable analytical tool for understanding why cybercrime thrives in Nigeria despite existing legislation. It shifts the discourse from reactive punishment to proactive prevention, emphasizing the importance of environmental and

[60] Ibid (n75).

structural interventions. By integrating this theory with the legal-institutional perspective, the study adopts a multidimensional framework that examines both the adequacy of Nigeria's cyber laws and the social conditions that facilitate digital criminality.[61]

**2.3 History of Cybercrimes in Nigeria**

The historical evolution of cybercrime in Nigeria reflects a gradual shift from isolated digital offenses to complex transnational criminal activities that necessitated a comprehensive legal response. Cybercrimes were first recognized as a significant national concern in the early 2000s, a period marked by the proliferation of email-based fraud schemes and internet scams that gained international notoriety. Hence, Nigeria became synonymous with "419" advance fee fraud a scheme in which individuals, often foreigners, were deceived into transferring money under the pretense of accessing larger returns, inheritances, or business opportunities.[62] Initially dismissed as sporadic acts of deception, the increasing frequency, sophistication, and global reach of these crimes soon revealed their economic and reputational consequences for the Nigerian state.

During this early phase, the Nigerian government faced growing diplomatic criticism and economic repercussions, as cyber fraud activities eroded investor confidence and tarnished the country's image abroad. Despite these challenges, early attempts to regulate cybercrime were fragmented and largely reactive. Legal instruments such as the Criminal Code Act and the Advance Fee Fraud and Other Fraud Related Offences Act of 2006 were applied in a limited manner to emerging cyber offenses. However, these traditional laws were never designed to handle the technical complexities of cybercrime such as hacking, phishing, or identity theft resulting in weak enforcement and frequent under-prosecution.[63]

---

[61] Ibid.
[62] H Muhammed, 'NCC Clamps Down on Illegal ISPs, Cyber Cafés' 2009 *Daily Trust*, 2 February, 55..
[63] A A. Akinsola, 'Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward (Pinheiro Legal Practitioners, 2021),' https://www.pinheirolp.com/articles/adapting%20to%20change_%20the%20

Law enforcement agencies during this period lacked both digital forensic capacity and specialized expertise, further hindering effective cybercrime investigation.[64] As a result, criminal elements exploited these institutional gaps to operate with near impunity, while the country's informal digital economy became increasingly susceptible to online manipulation and fraud. Accordingly, this early fragmentation in Nigeria's cyber-legal framework represented not only a failure of foresight but also a missed opportunity to align domestic laws with emerging international standards.[65]

A turning point came with the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which established the first comprehensive legal and institutional framework for combating cyber offenses in Nigeria. The Act consolidated previously scattered legal provisions and formally criminalized a wide range of digital activities, including hacking, cyberstalking, identity theft, cyberterrorism, child exploitation, and online financial fraud.[66] It also designated key agencies, such as the Office of the National Security Adviser (ONSA) and the Nigeria Computer Emergency Response Team (ngCERT), as central coordinators of national cybersecurity initiatives. Importantly, the Act mandated electronic data retention, facilitated international cooperation, and established the National Cybersecurity Fund to support enforcement and awareness programs.

However, the 2015 Act, while groundbreaking, also revealed the reactive nature of Nigeria's policy evolution[67]. It was enacted largely in response to escalating cyber incidents and external

---

impact%20and%20challenges%20of%20cybercrime%20in%20nigeria%20and%20the%20way%20forward.pdf, assessed October 2025; L. Ani, 'Cybercrime and National Security: The Role of the Penal and Procedural Law' (2015) *Law and Security in Nigeria* 197–231.

[64] J Sarum, 'Challenges and Solutions of Cybercrimes in Nigeria,' (2022) *International Journal of Academia Education* 1–43.

[65] Ibid (n50) 116.

[66] S Oho, '*A Critical Analysis of the Cybercrime Law in Nigeria,'* (Baze University, Abuja, 2017)

[67]Ibid (n99); P.T. Ortese, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective' (2023) *Benue State University Makurdi Law Journal* 12(1) 72–93.

pressure to conform with global cyber norms, including the Budapest Convention on Cybercrime and the African Union Malabo Convention on Cybersecurity and Personal Data Protection. Consequently, although the Act represented a major policy milestone, its reactive formulation meant it initially lacked mechanisms to address emerging technological threats such as cryptocurrency fraud, artificial intelligence enabled scams, and deepfake technology.

Overall, the historical trajectory of Nigeria's cybercrime regulation demonstrates a pattern of delayed institutional response to rapidly evolving digital threats. The prolonged absence of a coherent framework enabled cybercriminals to entrench themselves within local and transnational networks, while weak enforcement and limited inter-agency coordination hindered deterrence. Despite these shortcomings, the 2015 Act laid a crucial foundation for Nigeria's modern cybersecurity architecture. Nevertheless, the persistence of enforcement challenges, technological gaps, and socio-economic drivers of digital crime underscores the need for continuous legal reform, capacity building, and stakeholder collaboration to ensure that Nigeria's cyber laws remain adaptive to global and domestic realities.[68]

### 2.3.1 Regulatory Approaches to Cybercrime and Cybersecurity

Regulatory approaches to cybercrime and cybersecurity encompass the laws, institutional frameworks, policies, and enforcement mechanisms established by governments to prevent, detect, and punish cyber offenses. Given the borderless and complex nature of cyber threats, effective regulation demands a balance between technological innovation and legal oversight (Brenner, 2001). In the Nigerian context, this balance is pursued through both legislative and

---

[68] I J Fehintola, '*An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria,'* (Crescent University, Abeokuta, 2023); Y.A. Makeri, 'Cyber Security Issues in Nigeria and Challenges,' (2017) *International Journal of Advanced Research in Computer Science and Software Engineering* 7(4), 315–321; T I Akomolede and others, 'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism,' Paper Presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT), (2016) Nasarawa State University, Keffi.

strategic instruments, primarily the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and the National Cybersecurity Policy and Strategy (NCPS).[69]

The Cybercrimes Act, 2015 serves as Nigeria's principal legislation governing cyberspace. It criminalizes offenses such as cyberstalking, identity theft, unauthorized access, child pornography, and financial fraud, while establishing clear penalties for violations.[70] The Act further mandates critical institutions such as banks and telecommunication providers to report cyber incidents, retain relevant data, and cooperate with law enforcement agencies. The National Cybersecurity Fund, created under the Act, supports public awareness programs, capacity-building initiatives, and technological development in cybersecurity.

Complementing the Act is the National Cybersecurity Policy and Strategy (NCPS), first introduced in 2014 and revised in 2021. Coordinated by ONSA, the policy outlines Nigeria's vision for protecting critical national information infrastructure (CNII), fostering public–private partnerships, and enhancing human capacity for digital security management.[71] It emphasizes resilience, inter-agency cooperation, and international collaboration, recognizing cybersecurity as a strategic component of national security and economic development.

Institutionally, Nigeria's cyber regulatory ecosystem involves multiple agencies with distinct but interrelated mandates. The Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF) lead investigations and prosecutions of cyber-enabled financial crimes. The Nigeria Computer Emergency Response Team (ngCERT) under ONSA manages incident reporting and national cyber threat intelligence, while the National Information Technology Development Agency (NITDA) enforces data protection and IT compliance standards.

---

[69]S W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' (2001) *Murdoch University Electronic Journal of Law*, 8(2), 3–12.
[70] Ibid (n50) 104.
[71] Ibid (n46) 197–231.

Additionally, the Nigerian Communications Commission (NCC) regulates telecommunications networks to ensure operational security and compliance with cyber laws.[72]

On the international front, Nigeria aligns with several regional and global cybersecurity frameworks, including the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention, 2014), INTERPOL's African Cybercrime Initiative, and partnerships with organizations such as the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU). These collaborations enhance Nigeria's capacity for cross-border investigation, intelligence sharing, and technical skill development.[73]

Despite these advances, Nigeria's regulatory framework continues to face implementation challenges. Weak enforcement capacity, inadequate technical infrastructure, and limited coordination among agencies often undermine regulatory efficiency.[74] Overlapping institutional mandates sometimes lead to inter-agency rivalry, while low public awareness of cyber laws limits compliance among individuals and organizations. The absence of digital literacy and the prevalence of informal online activities exacerbate national cyber vulnerabilities.

To enhance regulatory effectiveness, Nigeria must adopt a proactive and adaptive governance approach strengthening technical capacity, harmonizing agency roles, and institutionalizing periodic legal reviews to reflect technological advancements. Equally important is the integration of cybersecurity education into national curricula and the promotion of a culture of digital responsibility. However, sustained investment in cybersecurity infrastructure, international

---

[72] A A Akinsola, 'Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward (Pinheiro Legal Practitioners, 2021), https://www.pinheirolp.com/articles/adapting%20to%20change _%20the%20 impact%20and%20challenges%20of%20cybercrime%20in%20nigeria%20and%20the%20way%20forward.pdf, assessed October 2025; I F Ibikunle, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution" (2013) *Department of Electrical & Information Engineering, Covenant University Nigeria* 1(1) 1..

[73] T I Akomolede and others, 'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism', paper presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT), (2016) Nasarawa State University, Keffi.

[74] Ibid (n96).

cooperation, and stakeholder engagement will be pivotal in ensuring that Nigeria's regulatory system keeps pace with emerging global cyber threats.[75]

Historically, Nigeria's journey toward effective cybercrime regulation has been shaped by reactive legal evolution, institutional fragmentation, and global pressure to conform with international standards. The Cybercrimes Act, 2015 and subsequent policy frameworks marked a significant leap forward, yet the continued rise of sophisticated digital crimes calls for dynamic, inclusive, and forward-looking reforms. Strengthening enforcement capacity, promoting awareness, and ensuring alignment with global best practices remain essential for securing Nigeria's digital future.

**2.4 Literature Review**

A wide range of scholarly literature has assessed the strengths and weaknesses of Nigeria's cybercrime legislation, especially focusing on the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. One of the leading voices, Kolawole, acknowledges the Act's pivotal role in codifying previously unregulated digital offenses such as identity theft, cyberstalking, and cybersquatting. Kolawole argues that this legal recognition represents a significant milestone in Nigeria's journey toward digital governance.[76] However, his critique centers on implementation gaps, noting that weak institution, underfunded regulatory agencies, and a lack of technical expertise within law enforcement and the judiciary undermine the Act's operational effectiveness. These challenges, he contends, render the law more symbolic than functional in many real-world cases.

[75] A Kolawole, 'Cybercrime Legislation in Nigeria: Effectiveness and Gaps,' (2022) *ResearchGate*, 1–6; P.T. Ortese, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective' (2023) *Benue State University Makurdi Law Journal* 12(1) 72–93.

[76]Ibid; Sahara Reporters (2023). ECOWAS Court Declares 'Nigeria's Cybercrime Act Section 24 Vague.

Fehintola, builds on this assessment by highlighting the practical enforcement challenges of the Cybercrimes Act. While comprehensive on paper, Fehintola argues that the law is not matched by operational readiness Nigeria lacks a robust digital forensics infrastructure, and investigators often do not possess the required technical know-how to build watertight cybercrime cases.[77] This concern is echoed in Sahara Reporters, which reports the ECOWAS Court's judgment that Section 24 of the Act, criminalizing cyberstalking is vague, arbitrary, and potentially unconstitutional. The court found that this provision infringed upon the right to freedom of expression, casting legal doubt on the validity of prosecutions carried out under it and reinforcing arguments for legislative reform.[78]

Nigeria's institutional and operational deficits in enforcing the law, Sarum, lists judicial incompetence in cyber-specific jurisprudence, poor inter-agency coordination, and ambiguity in the law's language as major stumbling blocks. Law enforcement personnel often depend on outdated training and obsolete digital tools, which make them ineffective in confronting sophisticated crimes like cryptocurrency fraud and transnational cyber threats. Similarly warns that many cybercrime cases collapse due to procedural lapses, weak evidence-gathering techniques, or misinterpretation of technical details.[79]

On the comparative front, provides insight into how other countries have strengthened their legal frameworks and institutional responses to cybercrime. Drawing lessons from the UK and the US, he emphasizes the importance of cyber intelligence units, digital forensic labs, and international partnerships, suggesting that Nigeria emulate these models. Other scholars, such as Nojeim and

---

[77]Ibid (n96).

[78] J Sarum, 'Challenges and Solutions of Cybercrimes in Nigeria,' (2022) International Journal of Academia Education 1–43; A A. Akinsola, "Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward (Pinheiro Legal Practitioners, 2021)" https://www.pinheirolp.com/articles/adapting %20to%20change_%20the%20mpact%20and%20challenges%20of%20cybercrime%20in%20nigeria%20and%20$^{th}$e%20way%20f orward.pdf, assessed October 2025.

[79] E Ogana, 'An Analysis of Legal Framework on Combating Cybercrime in Nigeria (Master's Dissertation, Ahmadu Bello University, Zaria, 2017) 17–214.

Brenner, raise important concerns about balancing cybersecurity enforcement with civil liberties. They warn that overly broad or ambiguous laws such as Nigeria's controversial Section 24 risk being misused to silence dissent or restrict online freedoms. Consequently, periodic legislative reviews, capacity-building for key justice actors, and the need for cybersecurity awareness campaigns. Olayemi, stresses the importance of collaboration between government and the private sector, especially telecom and fintech operators, to develop comprehensive cybersecurity resilience.[80] The Nigerian legal system has addressed some of these trends through notable court cases. For example:

- *Danfulani v. Economic and Financial Crimes Commission*,[81] the case examined the constitutionality of prolonged detention and the use of "holding charges" by the EFCC during investigations. The court emphasized that anti-corruption enforcement cannot override fundamental rights such as liberty and due process. It ultimately reinforced judicial scrutiny over EFCC detention procedures to prevent abuse of investigative powers.
- *Dasuki v. Federal Republic of Nigeria*,[82] this case centered on allegations of massive diversion of public funds and raised issues concerning the government's respect for court-ordered bail. The court stressed that even in high-profile corruption cases, the state must comply with constitutional protections and judicial decisions. It became a landmark for highlighting tensions between executive power and individual rights in anti-corruption prosecution.
- *Yanaty Petrochemical Ltd v. Economic and Financial Crimes Commission*, the Supreme Court held that a civil judgment does not bar the EFCC from conducting or reopening

[80] P T Ortese, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective' (2023) *Benue State University Makurdi Law Journal* 12(1) 72–93; T.I. Akomolede and others, 'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism', Paper Presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT), (2016) Nasarawa State University, Keffi.
[81] (2016) 1 NWLR (Pt 1493) 223.
[82] (2018) 10 NWLR (Pt 1627) 320

criminal investigations. It affirmed the Commission's broad statutory powers to investigate suspected financial crimes independently of civil proceedings. The ruling prevented the use of civil litigation as a shield against criminal accountability.

- *Economic and Financial Crimes Commission v. Diamond Bank Plc,* the court ruled that the EFCC must not be used as a debt-recovery or commercial dispute-resolution mechanism.[83] It clarified that the EFCC's mandate applies strictly to genuine economic and financial crimes rather than ordinary business disagreements. The decision protected the agency from being diverted into private commercial conflicts.
- *Alao v. Federal Republic of Nigeria*,[84] the court affirmed that the EFCC has independent prosecutorial authority, including in matters involving public procurement corruption. This clarification strengthened the Commission's legal autonomy from the Attorney General in criminal enforcement. It also provided doctrinal clarity on how different anti-corruption statutes interact in Nigeria.
- *Auwalu v. Federal Republic of Nigeria,* the judgment reinforced the EFCC's broad investigative and prosecutorial powers under its establishing Act.[85] It confirmed that the Commission may independently pursue financial-crime cases without relying on external direction. The case supports the institutional legitimacy of the EFCC while highlighting the need for safeguards against overreach.

### 2.4.2 Factors Influencing Cybercrime in Nigeria

[83] (2018) 8 NWLR (Pt 1620) 61.
[84] (2018) 10 NWLR (Pt 1627) 284.
[85] (2018) 8 NWLR (Pt 1620) 1.

Cybercrime in Nigeria is driven by a complex interplay of economic hardship, socio-cultural attitudes, weak institutional capacity, and technological vulnerabilities. While advancements in information and communication technologies (ICTs) have expanded digital connectivity, they have also exposed systemic weaknesses in cybersecurity governance, enforcement, and awareness. Major factors influencing cybercrime in Nigeria include poor cybersecurity infrastructure, inadequate forensic and surveillance tools, fragmented databases, cross-border investigative limitations, unemployment, and deficient public awareness.[86]

Weak Cybersecurity Infrastructure: Weak cybersecurity systems remain one of the most critical enablers of cybercrime in Nigeria. Many institutions, particularly in the public sector and among small-to-medium enterprises, lack adequate security protocols such as intrusion detection systems (IDS), anti-malware solutions, firewalls, and encryption tools.[87] The reliance on outdated software, irregular system audits, and low cybersecurity literacy among IT personnel make Nigeria's digital ecosystem vulnerable to exploitation. This vulnerability was illustrated in *Online Policy Group v. Diebold, Inc*, where hackers breached private email servers due to weak network defenses. The prosecution emphasized that the absence of proactive cybersecurity measures hindered early detection of the intrusion. Without substantial investment in digital infrastructure and the training of cybersecurity professionals, Nigeria remains exposed to recurrent attacks and systemic risks.[88]

Inadequate Tracking and Digital Forensics Capacity: Law enforcement agencies in Nigeria often lack access to advanced tracking devices, forensic tools, and digital surveillance technologies

---

[86] Ibid (n65).

[87] F Ibikunle, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution' *Department of Electrical & Information Engineering, Covenant University Nigeria* (2013) 1(1) 1.; Y.A. Makeri, "Cyber Security Issues in Nigeria and Challenges" (2017) *International Journal of Advanced Research in Computer Science and Software Engineering* 7(4), 315–321.; *Online Policy Group v. Diebold, Inc.,* (2003), No. C 03 03899, 337 F. Supp. 2d 1195 (N.D. Cal.)

[88] Y A, Makeri, 'Cyber Security Issues in Nigeria and Challenges,' (2017) *International Journal of Advanced Research in Computer Science and Software Engineering* 7(4), 315–321.

required to trace cybercriminal activities effectively. Agencies such as the Economic and Financial Crimes Commission (EFCC) and the Nigerian Police Force rely on outdated investigative methods, limiting their ability to collect admissible electronic evidence. This shortfall was evident in *Olagunju v. Federal Republic of Nigeria*,[89] where prosecutors failed to trace encrypted digital communications linking the suspect to online fraud. The urgent need to develop digital forensic laboratories, enhance investigative capacity, and foster public-private cooperation to combat technologically sophisticated cybercrime.[90]

Fragmented National Database Systems: The absence of an integrated national database significantly undermines cybercrime investigations. Systems such as the National Identity Number (NIN), Bank Verification Number (BVN), SIM registration, and voter data remain fragmented and non-interoperable.[91] This lack of integration allows cybercriminals to exploit loopholes, create multiple digital identities, and evade detection. Similarly, some databases impede effective cross-referencing of biometric and digital evidence, often leading to inconclusive investigations. Establishing a harmonized and centralized identity management system could enhance verification processes, deter digital impersonation, and strengthen forensic accuracy.

Jurisdictional and Cross-Border Constraints: Cybercrime's transnational nature complicates investigation and prosecution, particularly when offenders or data reside in foreign jurisdictions. Nigeria's limited mutual legal assistance treaties (MLATs) and inadequate cyber-diplomacy hinder international cooperation. This was highlighted in *United States v. Ivanov* is a landmark U.S. federal case where the court upheld extraterritorial jurisdiction over a Russian hacker who

[89] (2018) 10 NWLR (Pt 1627) 272. ace.soas.ac.uk

[90] I J Fehintola, *An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria* (Crescent University, Abeokuta, 2023).

[91] E Ogana, '*An Analysis of Legal Framework on Combating Cybercrime in Nigeria*,' (Master's Dissertation, Ahmadu Bello University, Zaria, 2017) 17–214.

never physically entered the United States but attacked U.S.-based computer systems. The court reasoned that because the harmful effects of Ivanov's conduct were felt within the United States, and Congress intended the relevant cybercrime statutes to apply extraterritorially, prosecution was proper. The decision is widely cited for establishing that cybercriminals operating abroad can still be subject to U.S. jurisdiction when their actions target or impact systems within the country.[92] To address such limitations, enhancing international partnerships, signing bilateral treaties, and improving cross-border cybercrime protocols is very important.[93]

Youth Unemployment and Socio-Economic Pressures: Socioeconomic hardship and youth unemployment significantly contribute to cybercrime. However, many Nigerian youths view cybercrime as a survival mechanism amid economic exclusion and job scarcity. This was reflected in *Federal Republic of Nigeria v. Ibrahim Usman*, where the defendant confessed to resorting to internet fraud following prolonged unemployment.[94] Addressing this issue requires economic empowerment programs, digital entrepreneurship initiatives, and vocational training to redirect technological skills toward legitimate innovation.[95]

Cultural Normalization and Lack of Digital Ethics: The glamorization of cybercrime in popular culture often through music, social media, and peer influence has normalized fraudulent behavior among young Nigerians.[96] Without structured digital ethics education or awareness programs, youths remain susceptible to criminal recruitment. In *Federal Republic of Nigeria v Fani-Kayode*, was a Court of Appeal decision addressing evidentiary standards in criminal prosecutions, particularly regarding proof of money-laundering offences. At page 512, the court emphasized

---

[92] *United States vs. Ivanov, 175 F. Supp. 2d 367* (D. Conn. 2001)
[93] P T Ortese, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective' (2023) *Benue State University Makurdi Law Journal* 12(1) 72–93.
[94] (2017) Suit No. FCT/HC/CV/8613/15,
[95] O J Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria' (2014) I*nternational Journal of Sociology and Anthropology* 6(3) 116–125.
[96] P Grabosky, '*Cybercrime: Problems of Classification and Conceptualization,'* (Cham Springer 2016).

that the prosecution must establish each element of the offence beyond reasonable doubt and cannot rely on suspicion or assumptions. The case is frequently cited for affirming that mere movement of funds, without clear proof of illicit origin or intent, is insufficient to secure a conviction.[97]

Reactive Rather Than Preventive Cybersecurity Policies: Nigeria's approach to cybercrime control remains reactive rather than preventive. Most interventions occurs post-incident, without systematic risk mapping or preemptive alerts. This reactive tendency was exposed in *Solomon Okedara v. Attorney General of the Federation*, the court held that although the provision limits freedom of expression, it is justified under Section 45 of the Constitution in the interest of public safety and order.[98] This decision demonstrates a reactive enforcement approach punishing harmful speech after it occurs rather than a preventive regulatory framework aimed at proactively safeguarding digital rights. Building early-warning systems, real-time monitoring platforms, and proactive awareness campaigns are vital for deterrence.

Limited Public Cyber Awareness: A significant segment of Nigeria's population lacks basic cybersecurity knowledge, making them easy targets for phishing, identity theft, and online scams. *Intel Corp. v. Hamidi,* California Supreme Court, USA, former employee sent mass e-mails criticizing Intel. While this is primarily a trespass-to-chattels case, the employees opened emails without recognizing potential risks or distractions, highlighting broader issues of digital literacy and awareness.[99]

---

[97] (2010) 14 NWLR (Pt. 1214) 481 at 512; L. E. Ani, 'Cybersecurity and Digital Rights in Africa' 2020 *Journal of African Law*,, 64(2), 112.
[98] (2019) CA/L/174/18,
[99] (2003), 30 Cal. 4th 1342 .

Poor Institutional Coordination: A lack of synergy among Nigerian cybersecurity agencies leads to inefficiency and data silos. According to Akomolede,[100] agencies such as the EFCC, NITDA, and NCC often operate independently, creating enforcement gaps. *Oluseun Olumide Fadele, Esq. v. Economic and Financial Crimes Commission*, In the FCT High Court upheld the applicant's fundamental rights, ruling that EFCC's threats of arrest and harassment in connection with his role in garnishee proceedings violated his constitutional liberties.[101] The court granted injunctive relief and awarded damages, emphasizing that even regulatory agencies must respect the rights and professional duties of legal practitioners.[102]

Weak International Cooperation: Finally, Nigeria's limited collaboration with international law enforcement agencies such as INTERPOL and Europol impedes the prosecution of cross-border cybercrimes. The importance of international cyber treaties and mutual legal assistance for evidence collection and extradition. In *Federal Republic of Nigeria v. Eze Dominic*, lack of cooperation with Foreign Service providers hindered access to vital digital evidence. Strengthening global partnerships and cyber diplomacy would improve transnational enforcement capacity.[103]

---

[100] T.I. Akomolede and others'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism', Paper Presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT), (2016) *Nasarawa State University, Keffi*.

[100] I J Fehintola, 'An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria,' (Crescent University Press 2023), 88.

[101] (2022) FCT/HC/GWD/CV /126/21 (High Court, FCT, Abuja, 4 April 2022).

**[102]**Ibid.

[103] *Federal Republic of Nigeria v. Eze Dominic* (2022); P.T. Ortese, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective' (2023) *Benue State University Makurdi Law Journal* 12(1) 72–93..

### 2.4.3 Conclusion of Literature

The reviewed literature reveals that while the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 represents a critical step toward addressing digital threats in Nigeria, its effectiveness remains significantly constrained by implementation challenges, legal ambiguities, and institutional weaknesses. Key concerns include the lack of trained personnel, poor investigative capacity, and outdated tools within law enforcement agencies, which hinder effective enforcement. Additionally, legal vagueness particularly evident in provisions like Section 24, has drawn judicial criticism, raising concerns over constitutional rights and freedom of expression.

Comparative insights show that more advanced jurisdictions have strengthened their legal and institutional frameworks through investment in digital forensics, inter-agency coordination, and international cooperation.[104] There is also a strong consensus that Nigeria's legal framework must be regularly updated to keep pace with emerging technologies such as cryptocurrency, artificial intelligence, and deep fake-enabled fraud. Importantly, balancing cybersecurity with civil liberties remains a critical consideration in developing effective and constitutionally sound cybercrime laws. The literature reveals a general consensus: although the Cybercrimes Act of 2015 was a crucial legislative advancement, its impact is severely limited by poor implementation, ambiguous provisions, institutional inefficiencies, and lack of synergy across enforcement and judicial bodies. To ensure the law's continued relevance and effectiveness, scholars recommend a combination of legal reform, judicial training, technological investment, public education, and international collaboration. These measures are vital if Nigeria hopes to effectively confront the dynamic and borderless nature of cybercrime in the digital age.

---

[104] O Chinedu, 'The Changing Dynamics of Cybercrime in Nigeria: Challenges and Responses' (2020) *Journal of African Security Studies* 15(2), 33–49.

## CHAPTER THREE

## LEGAL, INSTITUTIONAL FRAMEWORK AND ENFORCEMENT MECHANISMS FOR COMBATING CYBERCRIME

### 3.1 Introduction

In recognition of the dangers posed by cybercrime, the Nigerian government enacted the *Cybercrimes (Prohibition, Prevention, etc.) Act* in 2015, representing the country's first comprehensive legal instrument addressing cyber offenses. The Act criminalizes a wide range of activities, including cyberstalking, data breaches, identity theft, and cyberterrorism, while empowering key institutions such as the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), and the Office of the National Security Adviser (ONSA) to investigate and prosecute offenders. This legislation provides the foundation for Nigeria's cyber governance structure and reflects the state's alignment with global digital security standards. However, the effectiveness of this framework depends not only on institutional capacity and enforcement but also on the degree of public understanding and compliance with its provisions.[105]

Despite the existence of this legal architecture, public awareness of cybercrime laws in Nigeria remains significantly low, particularly in rural areas and among individuals with limited education or digital literacy.[106] Many citizens are unaware of the types of online activities that constitute criminal behavior under the *Cybercrimes Act*, nor do they understand the available mechanisms for reporting or seeking redress. This ignorance has led to both passive victimization where individuals fall prey to scams or identity theft, and inadvertent participation in unlawful acts, such as data breaches or misinformation dissemination. The digital divide, limited ICT education, and inadequate government-led sensitization campaigns have further

[105]Ibid (n50) 72–93.
[106] Ibid (n96).

deepened this awareness gap, weakening the preventive potential of the legal effective communication and public enlightenment are vital components of any policy framework that seeks to promote lawful digital engagement.[107]

The enforcement of cybercrime laws in Nigeria faces structural and institutional challenges that limit their practical impact. Although agencies such as the EFCC and NPF have established cybercrime units, they often lack adequate technical expertise, forensic tools, and inter-agency coordination. Judicial precedents such as *Federal Republic of Nigeria v. Osasuyi Aisosa*, Benin City and *Federal Republic of Nigeria v. Kingsley Nwosu*, Enugu, demonstrate successful prosecutions of online fraud and identity theft; however, these cases are relatively few compared to the scale of cyber offenses nationwide. The complexity of cybercrime investigations often involving cross-border data transfers and digital evidence requires specialized training and international cooperation, which remain underdeveloped within Nigerian law enforcement agencies. Consequently, many cases either go unreported or unresolved, diminishing public confidence in the system.[108]

### 3.2.1 Cybercrime (Prohibition, Prevention, etc.) Act, 2015

The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 serves as Nigeria's most comprehensive legislation for addressing modern digital threats and criminal activities. The Act outlines different categories of cyber offences, establishes institutional responsibilities, and provides a regulatory framework that aligns with global best practices in cybersecurity law. By setting out clear definitions and prohibitions, it ensures that harmful conduct within the digital

---

[107] Ibid (n107) 17–214; P. C. Agba, International Communication Principles, Concepts and Issues. In C. S. Okunna (Ed.), Techniques of Mass Communication: A Multi-Dimensional Approach. (Enugu: New Generation Books 2003), p. 9.

[108] (2019, FHC/B/CR/94/2019, Benin) and *Federal Republic of Nigeria vs. Kingsley Nwosu* (2021, FHC/EN/CR/132/2021, Enugu), and T I Akomolede and others,'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism', paper presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT) (2016) Nasarawa State University, Keffi.

space is actionable under Nigerian law, even when such conduct crosses borders or involves sophisticated technological tools.

Consequently, to criminal provisions, the Act establishes mechanisms for national coordination, promotes public–private cooperation, and places cybersecurity obligations on critical institutions. This holistic approach recognizes that cybercrime is not only a criminal justice issue but also a national security, economic governance, and social protection concern. The Act's structure reflects a deliberate effort to build a resilient legal system capable of adapting to evolving cyber risks.[109]

A. Criminalization of Core Cyber Offences (Sections 5–14): These sections collectively define the primary offences that constitute cybercrime under Nigerian law. They target unlawful access, interference with systems and data, the use of prohibited devices, and digitally enabled fraud. This categorization ensures that both direct attacks (such as hacking) and indirect or preparatory actions (such as the possession of malicious tools) are treated as criminal conduct. The provisions also impose liability for harmful online behaviour, including cyberstalking and harassment, recognizing the shifting nature of crime into social and psychological harm facilitated through digital spaces.

The structure of these sections underscores the law's preventive and punitive objectives. Preventive elements include criminalizing tools and behaviours that precede cyberattacks, while punitive elements address completed offences causing harm to individuals, institutions, and the state. The sections are drafted broadly enough to accommodate new forms of digital criminality while still providing clear actionable categories for prosecutors and investigators.[110]

[109] Chawki, M., Al-Alosi, H.M., & Shaaban, R. Cybercrime, Digital Forensics and Jurisdiction (Springer, 2015), 112.
[110] Ibid.

Section 6 – Unlawful Access (Hacking): Section 6 criminalizes unauthorized entry into computer systems, networks, or electronic devices, regardless of whether the intruder's intentions are malicious or exploratory. This section is designed to address the earliest stage of cybercrime penetration into a digital environment without permission. The law recognizes various forms of unauthorized access, including password cracking, bypassing access restrictions, and circumventing security firewalls. Even minimal or momentary unauthorized access can create vulnerabilities that compromise data confidentiality or allow placement of malicious software.[111]

The section's significance lies in its preventive power. By criminalizing unauthorized access itself, the law allows enforcement agencies to intervene before more serious harm occurs. The objective is to maintain trust in digital platforms by ensuring that both public and private systems remain protected against illicit intrusions. The provision therefore supports the broader national commitment to cybersecurity by deterring individuals from engaging in unauthorized digital exploration that could escalate into more severe offences.[112]

Section 8 – System Interference: Section 8 deals with deliberate activities that undermine the availability or functionality of computer systems. This includes actions such as overloading systems through Distributed Denial of Service (DDoS) attacks, altering system configurations to impair operations, or sabotaging infrastructure to cause service interruptions. These acts are particularly harmful because they can disable essential services in banking, telecommunications, healthcare, and governance. The importance of this section is heightened by the dependence of modern society on continuous digital operations. System interference has the potential to inflict

[111] A. O. Obalola and F. A. Omotayo, "Cybersecurity and Legal Framework in Nigeria: Analysis of the Cybercrime Act 2015" (2021) *African Journal of Law & ICT*, 9(2), 45–63.
[112] S. Brenner *Cybercrime and the Law: Challenges of the Internet* (Northeastern University Press, 2015).

large-scale damage, disrupt national infrastructure, and erode public trust in digital services.[113] By criminalizing such activities, the Act seeks to deter cybercriminals who target system availability and to preserve the stability of digital operations across critical sectors. Section 9; Unlawful Interference with Data: Section 9 focuses on protecting the integrity of data by criminalizing its unauthorized modification, alteration, deterioration, or deletion. This provision recognizes that data is a key asset in modern society, and manipulating it can cause long-term harm to individuals, financial institutions, or government agencies. Actions covered under this section range from tampering with electronic records, altering financial statements, to corrupting large databases. The provision further underscores the critical role of data integrity in governance, commerce, and personal identity representation. Digital evidence, financial transactions, and automated systems rely heavily on accurate data. Thus, unauthorized interference can have cascading effects, from financial losses to administrative paralysis. By criminalizing such conduct, the Act ensures accountability for harmful digital manipulations that undermine trust in electronic systems.[114]

Section 14; Cyberstalking: Section 14 addresses harmful online communication, including cyberbullying, harassment, threats, and unwanted electronic messages. This provision extends criminal liability to psychological and emotional harm inflicted via digital platforms. The section responds to the growing prevalence of abusive behaviour on social media, messaging apps, blogs, and email, recognizing that digital harassment can be as damaging as physical intimidation. The importance of this section lies in its protection of individual dignity, safety, and mental well-being. The Act acknowledges that cyberstalking can escalate into real-world harm or long-term

[113] Akintunde, I. & Nwankwo, C. *ICT Law in Nigeria: Regulation and Jurisprudence* (Hybrid Publishers, 2019).
[114] ibid

psychological distress. By criminalizing such behaviours, the law promotes responsible online conduct and provides victims with avenues for legal redress in the digital environment.[115]

Sections 13 & 15 – Computer-Related Forgery and Fraud: These sections deal with fraudulent or deceitful digital practices, including electronic forgery, manipulation of financial records, phishing, impersonation, and identity theft. The law acknowledges that digital technologies provide criminals with new methods to deceive individuals and institutions, often leading to significant financial loss. These sections serve as critical tools in combating cyber-enabled financial crimes, which represent a significant portion of cybercrime in Nigeria. By imposing heavy penalties, the Act aims to deter individuals who misuse digital systems to obtain illicit financial gain. The provisions also facilitate the prosecution of fraudsters who exploit gaps in electronic authentication and verification systems.[116]

Section 7 – Unlawful Use of Devices: Section 7 prohibits the creation, possession, procurement, or distribution of devices designed for committing cyber offences. These include malware, hacking tools, unauthorized access codes, and password crackers. The section targets preparatory conduct by criminals, acknowledging that the availability of such tools is often a precursor to cyberattacks. This preventive approach strengthens the nation's cybersecurity defence by reducing the circulation of tools that enable cybercrime. By criminalizing possession and distribution, even before actual harm occurs, the law curtails the resources available to cybercriminals and supports early intervention by law enforcement agencies.[117]

Protection of Critical Information Infrastructure (Sections 3 & 21–23): Section 3 empowers the President to designate specific computer systems or networks as Critical Information

---

[115] L. Odeh and U. Alhassan, "Reassessing the Effectiveness of the EFCC in Combating Financial Cybercrime in Nigeria" (2020).*Journal of Financial Crime*, 27(4), 1123–1140.

[116] Akintunde, I. & Nwankwo, C. *ICT Law in Nigeria: Regulation and Jurisprudence* (Hybrid Publishers, 2019).

[117] A. O. Obalola and F. A. Omotayo, "Cybersecurity and Legal Framework in Nigeria: Analysis of the Cybercrime Act 2015" (2021). *African Journal of Law & ICT*, 9(2), 45–63.

Infrastructure (CII). These include essential systems in financial services, telecommunications, transportation, energy, health, and government administration. Once designated, these infrastructures receive elevated legal protection due to their importance for national stability and public welfare. This section acknowledges that the disruption of certain digital systems could have catastrophic consequences for national security and economic continuity. By granting presidential authority to classify CII, the Act ensures that protective measures can be tailored to emerging risks. This empowers the government to respond swiftly to shifts in the digital threat landscape.[118]

Sections 21–23 – Duties and Protection Measures for CII Operators: Sections 21–23 impose strict obligations on operators of designated CII. These include implementing robust access controls, conducting regular cybersecurity audits, ensuring compliance with national cybersecurity standards, and reporting breaches promptly to regulatory authorities. These duties are designed to ensure that CII operators adopt best practices in cybersecurity management. The serious implications of disruptions to CII justify the increased regulatory oversight. These sections help reduce vulnerabilities in sectors where cyberattacks could trigger widespread service outages or national emergencies. They also promote accountability and preparedness by requiring operators to adopt a proactive approach to cybersecurity.[119]

Institutional Obligations of Financial Institutions (Sections 37–40): Section 37 mandates financial institutions to create comprehensive cybersecurity frameworks that can detect, monitor, and counteract cyber threats. These frameworks must align with internationally recognized standards and incorporate governance structures that ensure ongoing oversight of cybersecurity risks. This section highlights the vital importance of the financial sector in the digital economy.

---

[118] E. F. Ajayi, "Challenges to Enforcement of Cybercrime Laws in Africa" (2016) *Journal of African Law*, 60(1), 1–20.
[119] Ibid.

Given the high volume of electronic transactions and the complexity of financial systems, cyberattacks can result in significant economic losses. Mandatory cybersecurity programs help protect consumers, strengthen institutional resilience, and maintain trust in the financial system.

Section 38 – Mandatory Incident Reporting: Section 38 requires financial institutions to report suspicious cyber incidents or attempted breaches to the Central Bank of Nigeria (CBN) and relevant law enforcement agencies. This obligation ensures that authorities can respond swiftly and coordinate investigations to prevent further harm or systemic risks.[120]

The emphasis on reporting reflects the need for transparency in the financial ecosystem. Timely reporting allows regulators to assess vulnerabilities, identify emerging threats, and prevent broad-based attacks that could destabilize the financial system. Failure to report attracts penalties, underscoring the seriousness of this legal obligation. Section 39 – Retention of Traffic Data: Section 39 mandates that financial institutions retain traffic data and subscriber information to assist law enforcement in investigations. These records include transaction histories, communication logs, and digital footprints necessary for identifying offenders and reconstructing cybercrimes. Such retention is essential for ensuring the availability of digital evidence, which often determines the success of cybercrime prosecutions. Protecting this data from unauthorized access or tampering is equally crucial, as compromised data can hinder investigations and weaken the criminal justice process.[121]

Cybercrime Advisory Council (Section 41): Section 41 establishes the Cybercrime Advisory Council, comprising representatives from key security, regulatory, and policy institutions such as ONSA, EFCC, CBN, NCC, Nigeria Police, NITDA, and others. This inter-agency body is designed to bring together diverse expertise required for an effective national cybersecurity

[120] M. Chawki, H.M. Al-Alosi and R. Shaaban, *Cybercrime, Digital Forensics and Jurisdiction*. (Springer, 2015).
[121] Ibid.

strategy. The composition of the Council reflects the multi-dimensional nature of cybersecurity challenges. Each institution brings unique capacities financial oversight, intelligence, law enforcement, regulation, and technical knowledge allowing for a unified and informed national approach. This collaborative structure helps avoid fragmented or duplicative efforts.

Section 41; Functions: The Council's functions include advising the government on cybersecurity matters, developing national policies, coordinating inter-agency and international cooperation, and overseeing the implementation of the Cybercrime Act. It also promotes information sharing and ensures that Nigeria's legal framework evolves with changing technological landscapes. Through these responsibilities, the Council serves as the backbone of Nigeria's cybersecurity governance. It enhances national resilience by ensuring that stakeholders work collectively, align strategies with global standards, and adopt coordinated responses to emerging cyber threats.[122]

### 3.2.2 Economic and Financial Crimes Commission (EFCC) Act

Section 6 – Functions of the Commission: Section 6 assigns the EFCC responsibility for preventing, investigating, and prosecuting economic and financial crimes, including those facilitated through digital channels. As criminal activity migrates online, this section empowers the Commission to tackle cyber-enabled offences such as internet scams, online banking fraud, card fraud, and cryptocurrency-based schemes. This section is critical because financial cybercrime represents one of Nigeria's most prevalent and internationally visible cyber threats. Empowering the EFCC to address these offences reinforces national capacity to combat digital criminal networks and safeguard the financial system from exploitation.[123]

---

[122] S. Brenner, *Cybercrime and the Law: Challenges of the Internet* (Northeastern University Press, 2015).
[123] Ibid.

Section 7 – Investigative Powers: Section 7 grants the EFCC authority to trace suspicious transactions, freeze illicit accounts, seize assets, and conduct forensic investigations on digital devices. These powers are necessary for disrupting criminal operations early and recovering illicit proceeds from cybercrimes. With cybercriminals utilizing sophisticated digital tools and international networks, Section 7 ensures that the EFCC has both investigative reach and operational flexibility. It allows collaboration with financial institutions and telecom operators, enhancing the ability to track cybercriminal activities in real time.[124]

Sections 13 & 14 – Enforcement and Prosecution: These sections empower the EFCC to examine digital financial records and prosecute individuals or organizations involved in cyber-enabled financial crimes. The provisions emphasize cooperation with foreign agencies, recognizing that most cybercrimes have cross-border dimensions. Sections 13 and 14 reinforce the EFCC's role as Nigeria's primary agency for tackling financially motivated cybercrime. They support international collaboration and ensure that Nigeria complies with global enforcement standards, making it more difficult for criminals to evade justice.[125]

### 3.2.3 Independent Corrupt Practices and Other Related Offences Commission (ICPC) Act

Sections 12–19 – Corruption Offences: These sections address various forms of corruption, which today increasingly involve digital platforms. They apply to situations where corrupt individuals manipulate electronic procurement systems, alter electronic records, or exploit automated financial platforms for illicit enrichment. As public institutions digitize their operations, these provisions become more necessary to address cyber-enabled corruption. Digitalization has expanded the avenues through which corruption can occur, including through

[124] I. Akintunde and C. Nwankwo, *ICT Law in Nigeria: Regulation and Jurisprudence* (Hybrid Publishers, 2019).
[125] Ibid.

unauthorized system access or manipulation of electronic documentation.[126] Sections 12–19 provide the legal basis for prosecuting such misconduct, ensuring accountability in digital governance environments.

Section 26 – Forgery of Documents: Section 26 criminalizes the forgery of documents, including digital documents, certificates, licenses, and forms. This provision is essential in contemporary governance, where administrative processes, identity verification, and certifications are increasingly digital. By including electronic records under its scope, the section ensures that fraudulent manipulation of digital documents is treated as seriously as traditional forgery. This strengthens the reliability of digital governance systems and promotes trust in electronic transactions.[127]

Section 46; Interpretation Clause: Section 46 provides broad definitions that enable the Act to be applied effectively to modern technological environments. Courts can interpret terms such as "document," "record," or "property" to include digital formats, ensuring that corruption facilitated through ICT tools does not escape legal scrutiny. The provision also allows the Act to adapt to technological changes without requiring frequent legislative amendments. This ensures that as digital governance evolves, the ICPC retains the authority needed to combat corruption within electronic systems.[128]

### 3.2.4 The Criminal Code Act

Sections 419 & 418; False Pretence and Fraud: These sections remain relevant for prosecuting cyber-related frauds such as phishing, impersonation, and fraudulent digital solicitations. Despite being drafted before the digital age, their broad language enables their application to online fraud

[126] E. F. Ajayi, "Challenges to Enforcement of Cybercrime Laws in Africa" (2016) *Journal of African Law*, 60(1), 1–20.
[127] I. Akintunde and C. Nwankwo, *ICT Law in Nigeria: Regulation and Jurisprudence* (Hybrid Publishers, 2019).
[128] Ibid.

schemes. Courts have interpreted these provisions to address modern fraud committed through emails, social media, and electronic communication platforms. Their flexibility ensures that traditional deceit, when committed digitally, remains punishable.[129]

Sections 365–366 – Forgery: Sections 365 and 366 criminalize forgery, including the falsification of electronic signatures, digital documents, or electronic approvals. These provisions are particularly relevant in digital banking, e-commerce, and online authentication systems. By applying forgery laws to digital contexts, Nigerian courts ensure that the shift towards electronic documentation does not create loopholes for criminal activities. These sections complement modern cybersecurity provisions by preserving trust in electronic transactions.[130]

Sections 383–389; Stealing: These provisions criminalize stealing, which now includes unauthorized electronic fund transfers, digital asset theft, and misappropriation of e-wallet balances or cryptocurrency. The digital adaptation of these sections demonstrates the judiciary's flexibility in protecting intangible electronic assets. Their continued application ensures that theft, regardless of the medium, remains prosecutable. This supports the broader legal objective of safeguarding property in both physical and virtual environments.[131]

Sections 373–375; Defamation: Sections 373–375 apply to defamatory digital publications, including false or injurious content posted on social media, blogs, forums, or websites. These sections help address harmful online discourse that damages reputation. As digital communication becomes widespread, these provisions safeguard individuals and institutions from malicious online statements, reinforcing responsible digital expression.[132]

---

[129] A. O. Obalola and F. A. Omotayo, "Cybersecurity and Legal Framework in Nigeria: Analysis of the Cybercrime Act 2015" (2021). *African Journal of Law & ICT*, 9(2), 45–63.
[130] Ibid.
[131] Ibid.
[132] S. Brenner, *Cybercrime and the Law: Challenges of the Internet* (Northeastern University Press, 2015).

Sections 323–327; Threats and Intimidation: These sections criminalize threats and intimidation, including cyber harassment and digital extortion. They apply to messages sent through emails, social media, or encrypted platforms. The provisions ensure that the anonymity or reach of digital platforms does not shield offenders from accountability. By extending traditional criminal law into digital spaces, the Criminal Code continues to offer protection against harmful online conduct.

### 3.2.5 Other relevant laws and regulation

In addition to the major cybercrime-specific instruments, several other laws indirectly bolster Nigeria's cybersecurity ecosystem. The Criminal Code Act (applicable in the South) and the Penal Code Act (used in the North) criminalize offences such as fraud, impersonation, forgery, and the unauthorized use of another person's identity activities that often overlap with modern cybercrime. The Freedom of Information Act enhances transparency but includes provisions that penalize the misuse of official information or unlawful access to records, thereby contributing to information-security governance. The Digital Rights and Freedom Bill, though not yet enacted into law, seeks to expand protections for online privacy, digital expression, and data rights, while also ensuring responsible state surveillance and limiting potential abuses of power. Collectively, these laws complement existing cybersecurity regulations and help create a more robust, rights-respecting digital environment in Nigeria.[133]

## 3.3 Institutional Framework

The institutional framework for cybersecurity and cybercrime enforcement in Nigeria comprises a network of government agencies, regulatory bodies, and specialized units responsible for implementing laws, policies, and protective measures. These institutions coordinate efforts to

[133] N O Umejiaku and M.I Anyaegbu, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics In Nigeria,' (2016) *International Journal of Computers and Technology,* (15) (10), 1-10.

prevent, detect, and prosecute cybercrime, while also promoting awareness, capacity building, and adherence to national and international cybersecurity standards.

### 3.3.1 Nigeria Police Force (NPF)

The Nigeria Police Force plays a frontline role in investigating and prosecuting cybercrime across the country. Through its Cybercrime Unit, the NPF handles complaints related to hacking, online fraud, cyberstalking, and other digital offences. The unit is responsible for gathering digital evidence, conducting forensic analysis, and collaborating with both national and international partners to apprehend cybercriminals. The NPF also engages in public awareness campaigns to educate citizens about safe online practices, promoting preventive measures that reduce vulnerability to cyber threats. Its institutional capacity is continually strengthened through training in digital forensics, cyber investigation techniques, and the interpretation of electronic evidence.[134]

### 3.3.2 Economic and Financial Crimes Commission (EFCC)

The **EFCC** focuses on investigating and prosecuting cyber-enabled financial crimes, including internet fraud, online money laundering, and advance-fee scams. Its Cybercrime and Forensic Unit is specialized in tracing digital financial transactions, analyzing electronic data, and coordinating operations against cybercriminal networks. The EFCC also collaborates extensively with international law enforcement agencies such as INTERPOL and Europol to tackle transnational cybercrime, recover stolen assets, and prosecute offenders operating beyond Nigeria's borders. By combining legal authority with technical expertise, the EFCC ensures that cybercrime investigations are both comprehensive and enforceable.

### 3.5.3 Independent Corrupt Practices and Other Related Offences Commission (ICPC)

[134] F T Ngo and K. Jaishankar, 'Committing Crime in the Digital Age: The Criminological Landscape of Cybercrime' (2017) 11(1) *International Journal of Cyber Criminology* 1–20.

While primarily tasked with combating corruption in the public sector, the ICPC addresses cyber-enabled corruption through monitoring electronic systems, e-procurement platforms, and government databases. The ICPC investigates cases of digital record manipulation, unauthorized access to government ICT systems, and misuse of public resources via online platforms. It also promotes capacity-building initiatives in cyber governance, data integrity, and ICT compliance within public institutions. By ensuring that public digital infrastructures are secure and transparent, the ICPC indirectly supports Nigeria's broader cybercrime prevention framework.[135]

### 3.4 International Organizations

#### 3.4.1 INTERPOL

INTERPOL supports Nigeria by providing global intelligence networks, access to international criminal databases, and cybercrime alerts. Through its Cybercrime Directorate, INTERPOL coordinates multinational operations targeting cybercriminal groups that operate across borders. It offers training programs, forensic assistance, and digital investigation tools that enhance Nigeria's ability to track and identify perpetrators. The collaboration helps Nigeria respond to complex cybercrime cases involving international victims, foreign bank accounts, and cross-jurisdictional evidence. INTERPOL's role is crucial in combating internet fraud, ransomware, and financial cybercrime that exceed Nigeria's national investigative capacity.[136]

#### 3.4.2 AFRIPOL

AFRIPOL enhances African law enforcement cooperation by improving intelligence sharing, coordinating joint cybercrime operations, and providing technical training in digital evidence handling. By harmonizing legal and investigative standards across African states, AFRIPOL helps reduce safe havens for cybercriminals who exploit disparities in national legal systems. For

[135] S. Brenner, *Cybercrime and the Law: Challenges of the Internet* (Northeastern University Press, 2015).
[136] E. F. Ajayi, "Challenges to Enforcement of Cybercrime Laws in Africa" (2016) *Journal of African Law*, 60(1), 1–20.

Nigeria, AFRIPOL strengthens regional collaboration and supports the development of effective cybercrime strategies. This is particularly important for crimes involving neighbouring countries where cybercriminals often operate or hide. AFRIPOL's efforts contribute significantly to building a unified continental response to cyber threats.

### 3.5 Cybersecurity Practice in Nigeria

Cybersecurity practices in Nigeria encompass a combination of legal, institutional, technical, and educational measures aimed at safeguarding digital systems. Government agencies, private organizations, and critical infrastructure operators are mandated to implement robust security protocols, including firewalls, encryption, intrusion detection systems, and access controls. Regulatory agencies like the National Information Technology Development Agency (NITDA) provide guidelines for data protection, while the Nigerian Communications Commission (NCC) monitors telecommunications security standards. These coordinated efforts ensure that both public and private institutions adopt proactive measures to prevent cyber incidents.[137]

In addition to technical measures, Nigeria's cybersecurity practice emphasizes awareness, capacity building, and international cooperation.[138] Training programs for law enforcement, IT professionals, and public officials aim to strengthen digital forensics, incident response, and risk management capabilities. Public awareness campaigns educate citizens about phishing, online fraud, and safe social media use. Nigeria also participates in international initiatives, collaborating with INTERPOL, AFRIPOL, and other organizations to share threat intelligence, standardize cybersecurity practices, and respond effectively to cross-border cyber threats. Collectively, these practices reflect an evolving approach to cybersecurity that integrates legal

[137] INTERPOL, Global Cybercrime Trends Report 2023 (INTERPOL Digital Crime Unit, 2023).
[138] Ibid.

enforcement, institutional coordination, technological safeguards, and public engagement to enhance national resilience in the digital age.

# CHAPTER FOUR

# MAJOR LEGAL CHALLENGES AFFECTING THE ENFORCEMENT OF CYBERCRIME LAWS IN NIGERIA AND POSSIBLE SOLUTIONS

## 4.1 Introduction

The enforcement of cybercrime laws in Nigeria faces numerous legal challenges that undermine the effectiveness of existing frameworks and hinder the prosecution of offenders. Despite the enactment of the Cybercrime (Prohibition, Prevention, etc.) Act, 2015, and complementary statutes such as the EFCC Act and ICPC Act, gaps remain in addressing the complexity and transnational nature of cyber offences. Key challenges include outdated legal provisions in older statutes like the Criminal Code, jurisdictional ambiguities in cases involving cross-border cybercriminals, insufficient harmonization of national laws with international cybercrime conventions, and procedural hurdles in evidence collection and digital forensics. These issues are further compounded by limited awareness of cybercrime legislation among law enforcement agencies, inconsistent judicial interpretation, and inadequate technical capacity to investigate and prosecute sophisticated cyber offences effectively.[139]

Addressing these challenges requires a multifaceted approach that strengthens Nigeria's legal, institutional, and technological capacity to combat cybercrime. Possible solutions include reviewing and updating existing laws to reflect current technological realities, harmonizing domestic legislation with international cybercrime treaties, and clarifying jurisdictional authority in cross-border cases. Strengthening capacity-building initiatives for law enforcement officers, prosecutors, and the judiciary in digital forensics, cyber investigation, and evidence management is also critical. Additionally, enhancing public-private partnerships, investing in cybersecurity

[139] A Akinsola, 'Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward,' (2021) Pinheiro Legal Practitioners. Retrieved from https://www.pinheirolp.

infrastructure, and promoting awareness campaigns on cyber threats can improve compliance and cooperation in preventing cybercrime. By addressing both legal and operational gaps, Nigeria can create a more effective enforcement environment that deters offenders and safeguards individuals, institutions, and critical infrastructure in the digital space.

## 4.2 Challenges Affecting Enforcement

The enforcement of cybercrime laws in Nigeria faces significant challenges that hinder the effective prosecution and prevention of digital offences. Inadequate capacity among law enforcement agencies, including limited training in digital forensics, cyber investigation, and evidence management, weakens the ability to detect, investigate, and prosecute cybercriminals. Coupled with this are jurisdictional issues, as cybercrime often transcends national borders, creating complications in coordinating cross-border investigations and securing extradition of offenders. The rapid evolution of cyber threats further complicates enforcement, as emerging technologies such as cryptocurrencies, artificial intelligence, and sophisticated malware often outpace existing legislation. Lack of awareness and compliance among the public and organizations, ambiguous legal definitions, and loopholes in current statutes also contribute to gaps in enforcement, as many individuals and institutions remain uninformed about their obligations under the law or exploit unclear provisions to evade accountability.[140]

Additional challenges include corruption and bribery, which compromise the impartiality and effectiveness of law enforcement and judicial processes, allowing cybercriminals to manipulate or evade prosecution. Furthermore, the absence of standardized regulations across sectors and agencies creates inconsistencies in cybersecurity practices, enforcement priorities, and penalties for offences. These interrelated factors which create an environment where cybercriminals can

[140] I J Fehintola, *An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria* (Crescent University, Abeokuta, 2023).

operate with relative impunity, undermining national efforts to secure digital infrastructure, protect individuals and businesses, and maintain public trust in online systems are discussed as follows. Understanding these challenges is essential for developing practical solutions that strengthen enforcement, close legal gaps, and promote a coordinated and resilient cybersecurity framework in Nigeria.[141]

### 4.2.1 Weak Enforcement

The implementation of Nigeria's Cybercrime (Prohibition, Prevention, etc.), Act, 2015 has been hindered significantly by weak institutional capacity. Many law enforcement agencies, including the Nigerian Police Force, lack trained personnel capable of handling complex cybercrime investigations. Without foundational training in digital forensics and cyber intelligence, the provisions of the Cybercrime Act remain largely theoretical, resulting in poor enforcement outcomes.

Inadequate technical resources further compound this problem. Investigative units lack access to modern forensic tools, cyber incident response platforms, and real-time data monitoring systems. Cybercrime departments often work with outdated or no equipment, rendering them incapable of tracking advanced cyber threats effectively. This technological deficiency allows cybercriminals to operate with relative impunity.[142]

The judiciary, an integral part of cybercrime enforcement, is equally affected. Judges and legal practitioners often lack the technical understanding required to interpret digital evidence or assess cases involving evolving cyber mechanisms. This results in frequent delays, dismissals, or inconsistent rulings, ultimately undermining the credibility of the legal system in addressing cybercrime.

---

[141]Ibid (n127).
[142] Ibid (n128).

Akomolede et al., highlight the importance of specialized units and cross-sectoral collaboration, yet Nigerian agencies continue to function in isolation.[143] The lack of coordination between bodies like EFCC, DSS, NITDA, and the police weakens national response mechanisms. Jurisdictional overlaps and rivalry further erode trust and prevent the creation of a unified enforcement front. To enhance enforcement and capacity, sustained investment in human resource development, infrastructure, and multi-agency collaboration is essential. As Laura asserts, cybersecurity enforcement requires a technically adept, legally aware, and well-resourced institutional framework something Nigeria is yet to fully develop.

### 4.2.2 Inadequate Capacity

One of the foremost challenges in enforcing cybercrime laws in Nigeria is the limited capacity of law enforcement agencies. Effective cybercrime enforcement requires specialized knowledge and skills, including digital forensics, cyber investigations, network analysis, and proper evidence management. However, many law enforcement personnel lack adequate training in these areas, which significantly undermines their ability to detect, investigate, and prosecute cybercriminal activities. As a result, investigations are often incomplete, delayed, or ineffective, and the likelihood of securing successful convictions is reduced.[144]

The situation is further complicated by the rapid pace of technological change. Cybercriminals continuously adopt sophisticated methods ranging from encrypted communications and virtual currencies to artificial intelligence-driven attacks that can easily outstrip the existing knowledge and technical resources of law enforcement agencies. Without continuous professional

---

[143] T I Akomolede and others, 'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism', paper presented at the 47th Annual Conference of the Nigerian Association of Law Teachers (NALT) (2016) Nasarawa State University, Keffi.

[144] S W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law,' (2001) *Murdoch University Electronic Journal of Law* 8(2), 3–12.

development programs, officers struggle to keep pace with emerging threats, leaving critical gaps in enforcement.

Consequently, to training deficiencies, law enforcement agencies often face limited access to modern investigative tools, software, and hardware necessary for cybercrime detection and prosecution. Budget constraints and inadequate infrastructure exacerbate these challenges, preventing agencies from establishing fully equipped cybercrime units capable of handling complex cases. It is essential to invest in capacity-building initiatives, including targeted training programs, provision of modern investigative technologies, and the establishment of well-resourced cybercrime units. Strengthening technical expertise, operational efficiency, and investigative capabilities will enhance the ability of law enforcement to identify, investigate, and prosecute cybercriminals effectively, thereby reinforcing the overall cybersecurity framework in Nigeria.[145]

### 4.2.3 Jurisdictional Issues

Cybercrime's transnational nature makes it inherently difficult to manage within the confines of national legal systems. Nigeria’s attempts to prosecute cybercriminals often face challenges when the perpetrators or servers are located in foreign jurisdictions. As Olayemi, explains, cybercrimes transcend borders, and Nigerian law enforcement lacks the international reach or legal authority to gather cross-border digital evidence.[146]

A major obstacle lies in the country’s limited participation in mutual legal assistance treaties (MLATs) and its inadequate extradition framework. These limitations mean that even when a cybercriminal is identified abroad, Nigeria lacks the legal instruments to request cooperation or transfer suspects. The result is a persistent gap between identification and prosecution.

---

[145] Ibid (n127).
[146] Ibid.

Additionally, conflicting cyber laws across nations create inconsistencies in enforcement. What is considered criminal in Nigeria may not be illegal elsewhere, making harmonization difficult. The lack of international legal convergence makes it hard to prosecute cyber offenders who operate beyond national boundaries, using tools like VPNs and proxy servers to mask their identity.

The use of cloud storage and international social media platforms poses further challenges. For instance, obtaining data from companies headquartered in the United States or Europe involves complex legal and diplomatic processes, delaying investigations. Nigerian investigators frequently encounter resistance when attempting to access critical evidence stored abroad.[147] To address these jurisdictional issues, Nigeria must strengthen its engagement in international cybercrime conventions such as the Budapest Convention and build bilateral agreements with key countries. Also fostering cross-border cooperation and data-sharing arrangements is imperative to bridge jurisdictional gaps in cybercrime enforcement.[148]

### 4.2.4 Evolving Cyber Threats

Cybercriminals are constantly adopting innovative methods to exploit weaknesses in digital infrastructure. The emergence of sophisticated tools like ransomware, phishing kits, deepfakes, and AI-powered malware has outpaced Nigeria's legal framework. The Cybercrime Act, though comprehensive in 2015, lacks sufficient coverage for several modern threats, leaving legal grey areas. **T**he need for computational intelligence in cyber defense, yet Nigeria has been slow to adopt such technologies in both the public and private sectors. Most institutions lack predictive

[147]Y A Makeri, 'Cyber Security Issues in Nigeria and Challenges,' (2017) *International Journal of Advanced Research in Computer Science and Software Engineering* 7(4), 315–321.

[148] Ibid (n131); D Dasgupta, 'Computational Intelligence in Cyber Security,' in *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (CIHSPS 2006) 2–3.

analytics tools and threat intelligence frameworks that could help preempt or mitigate cyberattacks. This technological lag provides cybercriminals with a distinct advantage.

In addition, cyber threats are becoming more organized. Groups now operate in syndicates, with specialized roles ranging from coding to laundering funds using cryptocurrency. This level of specialization has made traditional crime-fighting techniques obsolete. As Jain notes, cybercrime is no longer a solo activity it involves networked operations that require coordinated countermeasures. Furthermore, the country's response to emerging threats remains reactive rather than proactive. Consequently, legislative reform takes too long, and policy innovation is limited. This leaves Nigeria vulnerable to new waves of cyberattacks that the current legal and security apparatus cannot adequately address.[149]

To tackle evolving cyber threats, Nigeria needs a dynamic legal framework, continuous technological upgrades, and an agile cybersecurity strategy. As Ibikunle recommends, consistent review of the law and strategic investment in research and development are key to staying ahead of cybercriminals.[150]

### 4.2.5 Lack of Awareness and Compliance

One of the core vulnerabilities in Nigeria's cybersecurity ecosystem is the widespread lack of awareness among citizens, businesses, and even government personnel. Many users do not understand basic cybersecurity hygiene such as password protection, phishing avoidance, or software updates. This ignorance creates fertile ground for cybercriminals to exploit unsuspecting users. The issue is compounded by poor cybersecurity culture in small and medium-sized enterprises (SMEs), many of which fail to implement basic safeguards. According

[149] A Kolawole, 'Cybercrime Legislation in Nigeria: Effectiveness and Gaps,' (2022) *ResearchGate*, 1–6.
[150] D Dasgupta, 'Computational Intelligence in Cyber Security,'; (2016); F Ibikunle, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution' (2013) *Department of Electrical & Information Engineering, Covenant University Nigeria* 1(1) 1.

to Fehintola[151] most SMEs do not prioritize cybersecurity in their operations due to cost, ignorance, or the misconception that they are not targets for attacks. This exposes them to attacks like ransomware, business email compromise, and identity theft.

However, government agencies and institutions often operate outdated systems, making them easy targets. Nigeria's struggles in regulating cyber cafes and ISPs an issue that persists today, especially in informal digital spaces. Public institutions also rarely report data breaches or comply with cybersecurity policies due to the absence of mandatory compliance mechanisms.[152]

Another layer of the problem is the minimal emphasis placed on cybersecurity education. Communication plays a vital role in shaping public behavior. Yet, there are very few public campaigns or educational initiatives to increase digital literacy in schools and communities. The result is a population largely unprepared to navigate the digital environment safely. To mitigate these challenges, Nigeria needs to launch a nationwide cyber-awareness campaign. As Sarum suggests, digital safety education should be integrated into school curricula and professional development programs to cultivate a more resilient digital society.[153]

Cybercrime investigations often walk a fine line between protecting public interest and safeguarding individual rights. In Nigeria, law enforcement practices sometimes violate constitutional protections due to inadequate oversight. Section 24 of the Cybercrime Act has been widely criticized and even ruled unlawful by the ECOWAS Court for being overly vague and arbitrarily enforced.[154]

---

[151] Ibid (128).
[152] H Muhammed, 'NCC Clamps Down on Illegal ISPs, Cyber Cafés,' 2009 *Daily Trust*, 2 February, p. 55.
[153] J Sarum, 'Challenges and Solutions of Cybercrimes in Nigeria,' (2022) *International Journal of Academia Education* 1–43.
[154] Sahara Reporters, 2023. 'ECOWAS Court Declares Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful' (22 March 2023). https://mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/ assessed November 2025.

Surveillance without proper judicial authorization raises ethical questions about privacy and due process. While cybersecurity measures are necessary to prevent terrorism and serious crime, unchecked surveillance can lead to mass data collection and abuses of power. Nigeria's lack of a comprehensive data protection framework further exacerbates these concerns.

The use of the Cybercrime Act to suppress dissent or silence journalists has also been reported. Critics argue that rather than serving solely as a tool for combating cyber threats, the Act is sometimes weaponized to curtail freedom of speech, especially on social media platforms. There are also concerns about the admissibility and protection of personal data collected during investigations. Without proper legal safeguards, individuals' information can be mishandled, leaked, or exploited, violating the right to privacy. This issue is especially troubling in cases involving sensitive personal or financial information.[155]

To uphold ethical standards, Nigeria must revise ambiguous sections of the Cybercrime Act and enact a robust data protection law. Independent oversight bodies and civil society engagement are essential to ensure accountability and transparency in cybersecurity operations.[156]

### 4.2.6 Ambiguous Definitions and Legal Loopholes

The Cybercrime (Prohibition, Prevention, etc.) Act of 2015, while a landmark in Nigerian legal development, suffers from ambiguous definitions that have led to inconsistent interpretation and enforcement. For instance, terms like "cyberstalking," "cyberbullying," and "hate speech" are broadly worded, allowing for wide discretion in interpretation. Such vagueness creates room for selective enforcement, abuse of power, and wrongful prosecution.

---

[155] F T Ngo and K Jaishankar, 'Committing Crime in the digital Age: The Criminological Landscape of Cybercrime,' (2017) *International Journal of Cyber Criminology* 11(1), 1–20.

[156] E Ani, 'Cybersecurity and Digital Rights in Africa' (2020) *Journal of African Law*, 64(2), 112.

One of the most criticized sections is Section 24, which criminalizes messages deemed "grossly offensive" or causing "annoyance." The ECOWAS Court ruled in *Sahara Reporters* of 2023[157] that this section is vague and arbitrary, highlighting the dangers of poorly defined legal boundaries. The ruling underscored how ambiguous laws can infringe on constitutionally guaranteed rights like freedom of expression.

Similarly, legal loopholes in the Act also create challenges for effective implementation. For example, the Act lacks clarity on intermediary liability whether internet service providers or platforms like Facebook and WhatsApp are responsible for third-party content. This uncertainty complicates law enforcement's efforts to prosecute cybercrime committed using these platforms.[158]

Moreover, the lack of judicial precedent and interpretive consistency means that judges often interpret the law based on limited understanding or context, leading to divergent legal outcomes. Therefore, the procedural and penal dimensions of cybercrime law must be clarified to eliminate confusion among legal practitioners and reduce wrongful application. To resolve these issues, a comprehensive review of the Cybercrime Act is necessary. Lawmakers must revise vague provisions, provide clear definitions, and align the legislation with international best practices. Legislative clarity will improve both enforcement and judicial confidence while ensuring citizens' rights are protected.

### 4.2.7 Corruption and Bribery

Corruption and bribery remain endemic problems in Nigeria's law enforcement sector, and they significantly hinder the fight against cybercrime. Officers tasked with investigating cyber

[157] 'ECOWAS Court Declares Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful' (22 March 2023),' https://mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/ assessed November 2025.

[158] I E Nwaobilo and U C Umearokwu, 'Cybersecurity as a National Concern: Implications for Nigeria's Digital Economy,' (2024) *Nigerian Journal of Information Security Studies* 3(1) 21–39.

offenses are sometimes susceptible to bribes from perpetrators, leading to the compromise or abandonment of cases. This undermines public trust in the legal system and emboldens cybercriminals.

Cybercrime investigations, due to their complexity and time requirements, often depend on individual officers' diligence and moral compass. When corrupt practices intervene, investigations are stalled, manipulated, or closed prematurely. In some cases, suspects are released without trial, and victims receive no justice.

Bribery also affects prosecution and judicial outcomes. Legal practitioners may collude with law enforcement or court officials to distort proceedings in favor of suspects. Corruption in financial cybercrime cases especially involving influential individuals or entities often results in minimal or no accountability. Additionally, internal monitoring and accountability structures within law enforcement agencies are weak or absent. There is little deterrence against corrupt officers, and whistleblowers often face retaliation rather than protection. This culture of impunity exacerbates the problem, especially in cybercrime units where oversight is minimal. To address these challenges, Nigeria must establish strong internal affairs units, implement anti-corruption training within cybercrime departments, and enforce whistleblower protections. The integrity of cybercrime enforcement depends on the ethical conduct of institutions entrusted with public trust.[159]

### 4.2.7 Lack of Standardized Regulations

The absence of standardized regulations and cybersecurity benchmarks has created a fragmented and underdeveloped digital defense environment in Nigeria. Many institutions operate without clearly defined cybersecurity policies, making it difficult to ensure data protection, respond to

[159] Ibid (n128); F Ibikunle, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution,' (2013) *Department of Electrical and Information Engineering, Covenant University Nigeria* 1(1) 1.

incidents, or coordinate with regulatory agencies.[160] While the Cybercrime Act provides a general legal framework, it does not specify operational standards for data encryption, incident reporting, risk assessment, or infrastructure resilience. Consequently, different sectors adopt inconsistent cybersecurity practices, leading to uneven protection and vulnerabilities across public and private entities. Nikhita and Ugander, stress the importance of establishing national standards that define roles, protocols, and compliance requirements for all digital actors. In Nigeria, however, there is limited enforcement of security standards, and bodies like NITDA and NCC lack full regulatory authority or alignment with the Act. This has made cybersecurity policy implementation slow and disjointed.[161]

Another issue is the lack of mandatory reporting mechanisms for data breaches. Organizations are not compelled to report cyberattacks or disclose compromised information. This hinders national threat intelligence efforts and weakens Nigeria's overall cyber resilience. Without a unified approach, even major cyber incidents can go undetected or unaddressed at the national level. To resolve this, Nigeria must develop comprehensive cybersecurity regulations, aligned with international standards such as ISO/IEC 27001. Effective cyber governance requires a standardized legal and operational framework that cuts across sectors and ensures compliance through audits, sanctions, and incentives.

[160] I F Ibikunle, "Approach to Cyber Security Issues in Nigeria: Challenges and Solution' (2013) *Department of Electrical and Information Engineering, Covenant University Nigeria* 1(1) 1.

[161] R G Nikhita and G J Ugander, 'A Study of Cybersecurity Challenges and Its Emerging Trends on Latest Technologies,' (2020) *International Journal of Innovative Science and Research Technology* 1–5.

# CHAPTER FIVE

# SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSION

## 5.1 Summary of Findings

**This study did an analysis of the effectiveness of cybercrime laws in Nigeria: Challenges and solutions, the summary of findings revealed that:**

1. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 is the cornerstone of Nigeria's legal response to cyber-related offenses. It was introduced to address the growing threat of cybercrime in a rapidly digitizing society. The Act criminalizes a broad range of offenses including cyberstalking, cybersquatting, identity theft, phishing, online fraud, and distribution of child pornography. It also establishes procedures for the investigation and prosecution of cyber offenses and mandates the protection of Critical National Information Infrastructure (CNII). In addition, the Act introduces obligations for service providers to retain user data and cooperate with law enforcement agencies during investigations. These provisions demonstrate a commendable attempt to align Nigeria's legal landscape with international norms and digital realities.
2. Despite its comprehensive outlook, the Act falls short in addressing newer and more sophisticated forms of cyber threats. The pace of technological innovation such as the rise of cryptocurrency-related crimes, ransomware attacks, AI-driven deepfakes, and cyberterrorism has outstripped the scope of the law. The absence of specific provisions for these emerging threats leaves enforcement agencies with limited tools to tackle them effectively. Furthermore, the law has not undergone substantive revision since 2015, which raises concerns about its responsiveness to dynamic cyber environments. One of the most controversial elements of the Act is Section 24, which addresses cyber harassment and offensive messages. Critics argue that the language of this section is overly broad and vague,

enabling its misuse against journalists, activists, and ordinary citizens exercising free speech online. Several cases have emerged where Section 24 was used to silence dissent or criticism of public officials, drawing criticism from civil society and human rights organizations.[162]

3. Thus, while the Act marks a major milestone in Nigeria's cyber law development, its long-term effectiveness is constrained by outdated language, a lack of specificity regarding modern threats, and human rights concerns. A comprehensive amendment is necessary to realign the legislation with technological trends, international best practices, and constitutional safeguards. Public awareness is an essential component of any effective cybersecurity strategy, but in Nigeria, awareness levels remain alarmingly low. Research indicates that most citizens, including business owners, students, and civil servants, lack basic knowledge of cyber laws and safe digital practices. This ignorance extends to understanding how to recognize, report, or respond to cyber incidents. As a result, many crimes go unreported, and victims are left without recourse or understanding of their legal rights.
4. The digital divide further complicates awareness efforts. While urban populations have relatively better access to information, rural communities where digital penetration is lower receive limited education on cybercrime prevention. This geographic disparity results in uneven levels of cyber literacy, leaving a large portion of the population vulnerable to online fraud, phishing scams, and identity theft. Informal internet users, particularly young people and market traders, are frequent targets of cybercriminals due to their limited knowledge and lack of preventive measures. Efforts by agencies such as the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission

[162] Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015;* Cybercrimes (Prohibition, Prevention, etc.) Act. (2015). *Cybercrime law enacted by the National Assembly of the Federal Republic of Nigeria*

(NCC) to educate the public have seen some success, particularly through workshops and online campaigns. However, these initiatives remain underfunded, inconsistent, and rarely translated into indigenous languages. They also tend to focus on urban centers, thereby neglecting rural audiences who are equally, if not more, vulnerable.

5. The enforcement of cybercrime laws in Nigeria is primarily the responsibility of agencies such as the Nigerian Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), and the Office of the National Security Adviser (ONSA). Each of these institutions has a role to play in investigating, preventing, and prosecuting cyber offenses. Over the years, specialized units like the EFCC's Cybercrime Section and the NPF Cybercrime Unit have been established to handle complex digital cases. However, their efforts are often hampered by systemic challenges, including inadequate funding, outdated infrastructure, and lack of trained personnel.
6. Cybercrime investigations require sophisticated tools and technical expertise, yet many enforcement agencies operate with rudimentary resources. Inadequate digital forensic labs, poor internet connectivity, and lack of data analytics capacity hinder their ability to trace and document cybercriminals' digital footprints. Additionally, law enforcement personnel often lack the training necessary to understand and handle digital evidence, leading to frequent procedural errors and poor case outcomes in court. Another major shortfall lies in the judiciary, which struggles with the interpretation and application of cyber laws. Many judges have limited exposure to digital technology, making it difficult to understand technical evidence and rule effectively on cybercrime matters. This judicial gap leads to protracted trials and low conviction rates. The lack of court-recognized experts in digital forensics further weakens the judicial process.

7. Compounding these issues is the lack of inter-agency coordination. Cases involving cybercrime often span multiple jurisdictions and require a multidisciplinary response. However, poor collaboration between agencies often leads to duplication of efforts, jurisdictional disputes, and fragmented investigations. For example, law enforcement may investigate a cyber-fraud case without consulting the Central Bank of Nigeria (CBN) or relevant financial institutions, thereby missing critical leads.
8. To improve enforcement, there is an urgent need to invest in digital infrastructure, strengthen inter-agency cooperation, and build the capacity of law enforcement and judicial officers. Without these structural reforms, the gap between law and enforcement will continue to widen, allowing cybercriminals to act with impunity. The enforcement of cybercrime legislation in Nigeria is hindered by multiple legal and procedural challenges. One major issue is the ambiguous wording in certain sections of the Cybercrime Act, especially Section 24. The lack of clarity regarding what constitutes "offensive messages" or "cyberstalking" has led to inconsistent interpretations and selective application of the law. This ambiguity not only undermines the rule of law but also poses a threat to constitutionally protected rights, such as freedom of expression and privacy.
9. Another challenge lies in the evidentiary standards required for prosecuting cybercrimes. Courts demand a high level of technical precision in collecting, storing, and presenting digital evidence. However, Nigeria lacks standardized protocols and a national digital forensics policy. As a result, many cases collapse due to inadmissible evidence or failure to establish proper chain of custody. This weakness is further exacerbated by a shortage of qualified forensic experts and inadequate training for prosecutors. Jurisdictional limitations also pose a significant obstacle. Cybercrimes often involve perpetrators and servers located

outside Nigeria, making it difficult to apprehend or prosecute offenders. Nigeria has yet to enter into comprehensive mutual legal assistance treaties with many countries, and it is not a signatory to key international instruments like the Budapest Convention on Cybercrime. This limits international cooperation and complicates transnational investigations. Corruption within law enforcement and judicial agencies further compounds these problems.

### 5.2 Recommendations and Solutions

1. Periodic review and amendment of the Cybercrime Act to include modern cyber threats such as AI, cryptocurrency scams, and deepfakes. Sections that are vague, particularly those that threaten digital rights, should be redefined with clearer language.
2. Launch nationwide, multilingual cybercrime awareness programs via traditional media, social media, and grassroots outreach. Engage religious and community leaders to disseminate messages in rural areas.
3. Invest in the training of law enforcement agents, prosecutors, and judges on digital forensics, cyber law, and electronic evidence management. Establish cybercrime labs in collaboration with academia and the private sector.
4. Develop and adopt protocols for the admissibility of digital evidence in court, ensuring that data is collected and preserved in accordance with global best practices.
5. Implement robust anti-corruption frameworks within law enforcement and judiciary systems, including internal audits, complaint reporting systems, and public oversight bodies.[163]
6. Strengthen cross-border partnerships through mutual legal assistance treaties and alignment with international cybercrime frameworks such as the Budapest Convention.

[163] S.W. Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' *Murdoch University Electronic Journal of Law* (2001) 8(2) 3–12.

Possible Solutions

**Strengthening Law Enforcement Capacity: Effective cybercrime enforcement in Nigeria requires building the technical and operational capacity of law enforcement agencies. This involves providing specialized training in digital forensics, cyber investigations, and evidence management, as well as equipping officers with modern investigative tools, forensic software, and cyber intelligence platforms. Establishing dedicated cybercrime units with autonomy, specialized resources, and trained personnel, along with institutionalized inter-agency collaboration between bodies like the EFCC, NCC, and DSS, would enhance efficiency and ensure swift prosecution of cybercriminals. Sustained investment in capacity-building programs and cybersecurity infrastructure is critical to achieving long-term effectiveness.**

**Promoting International Cooperation: Given the transnational nature of cybercrime, Nigeria must engage in robust international partnerships. Participation in global frameworks such as the Budapest Convention, establishing mutual legal assistance treaties (MLATs), and joining platforms like INTERPOL's I-24/7 or Europol's EC3 would facilitate cross-border investigations and data sharing. Bilateral collaboration with countries hosting major technology firms, alongside a competent foreign cyber liaison team, would streamline compliance with data requests and align Nigeria's cyber strategy with international best practices. International training programs also provide exposure to global standards and investigative techniques.**

**Updating Legislation and Raising Public Awareness: Cybercrime laws must evolve to address emerging threats such as AI-driven fraud, cryptocurrency scams, and deepfakes.**

**Updating the Cybercrime Act and related regulations would clarify legal definitions, close loopholes, and outline stakeholder responsibilities for financial institutions, telecom providers, and digital platforms. Public awareness campaigns targeting individuals and businesses, particularly SMEs, are equally vital. Educating citizens about cybersecurity practices, legal protections, and reporting mechanisms, while promoting compliance and digital hygiene, strengthens national resilience and encourages cooperation with law enforcement.**

**Integrating Ethics, Collaboration, and Evidence Management: Cybercrime enforcement must balance security with human rights, ensuring surveillance, data collection, and investigations respect privacy and due process. Training law enforcement in digital ethics, establishing independent oversight, and promoting public-private collaboration enhance trust, information sharing, and rapid response to threats. Standardized digital evidence protocols, including chain-of-custody procedures and forensic validation, improve prosecutorial outcomes and ensure admissibility in court. Engaging academia, tech communities, and ethical hackers further strengthens intelligence gathering and system protection.**

**Combatting Corruption, Promoting Cybersecurity Education, and Encouraging Ethical Hacking: Addressing corruption within law enforcement and enhancing transparency are essential for effective cybercrime prosecution. Digital tools, independent complaint channels, and cross-agency oversight reduce opportunities for misconduct and increase public confidence. Parallel efforts in cybersecurity education, professional training, and research centers cultivate a skilled workforce capable of responding to threats. Additionally, legitimizing ethical hacking and establishing national bug bounty programs**

**incentivize proactive vulnerability detection, harness local talent, and foster a culture of cybersecurity innovation across public and private sectors.**

## 5.3 Conclusion

The enactment of the Cybercrimes (Prohibition, Prevention, etc.), Act, 2015 marked a significant milestone in Nigeria's fight against digital crime. However, its effectiveness is hindered by structural, legal, and operational shortcomings. Low public awareness, poor enforcement capacity, outdated legal provisions, and weak institutional coordination continue to plague Nigeria's cybersecurity landscape. To combat these challenges, a multi-pronged approach involving legislative reform, public education, institutional strengthening, and international cooperation is urgently needed. If these recommendations are implemented, Nigeria will be better positioned to protect its digital ecosystem, ensure justice for victims, and deter cybercriminals effectively.

**Bibliography**


Advances in User Authentication. Springer (2018).

Agba C, 'International Communication Principles, Concepts and Issues." *Techniques of Mass Communication: A Multi-Dimensional Approach*,' (edited by C. S. Okunna, New Generation Books, 2003)

Ajayi, E. F. "Challenges to Enforcement of Cybercrime Laws in Africa" (2016) *Journal of African Law*, 60(1), 1–20.

Akindipe T and Akilla, O, 'Penal and Procedural Dimensions of Cybersecurity Enforcement in Nigeria,' *Nigerian Law and Technology Review*, (2024) 5( 1),

Akinsola A, *Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward*. Pinheiro Legal Practitioners, 2021. Accessed Oct. 2025.

Akintunde, I. and Nwankwo, C. *ICT Law in Nigeria: Regulation and Jurisprudence* (Hybrid Publishers, 2019).

Akomolede TI and others, 'Cybercrime and Cybersecurity as Challenges to the Fight Against Global Terrorism,' 47th Annual Conference of the Nigerian Association of Law Teachers (NALT), Nasarawa State University, Keffi, 2016.

Ani E, 'Cybersecurity and Digital Rights in Africa." *Journal of African Law*, (2020) 64 (2).

Ani L, 'Cybercrime and National Security: The Role of the Penal and Procedural Law,' *Law and Security in Nigeria* (2015).

Balogun, Folake. "Nigerian Organisations Recorded 4,388 Attacks per Week in Q1 Check Point" 17 Apr. 2025.*BusinessDay*,

Brenner S W, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law,' *Murdoch University Electronic Journal of Law* (2001) (8) (2),

Brenner, S. *Cybercrime and the Law: Challenges of the Internet* (Northeastern University Press, 2015).

Chawki,M., Al-Alosi, H.M. and Shaaban, R. *Cybercrime, Digital Forensics and Jurisdiction*. (Springer, 2015).

Chinedu O, 'The Changing Dynamics of Cybercrime in Nigeria: Challenges and Responses,' *Journal of African Security Studies* (2020) (15) (2)

Clough J *Principles of Cybercrime*. Cambridge University Press, 2015.

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria).

Cybersecurity Ventures. *2024 Official Cybercrime Report*. 2024.

Cybersecurity. Springer 92019).

Dasgupta D, 'Computational Intelligence in Cyber Security." *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (CIHSPS 2006).

Economic and Financial Crimes Commission v. Olumide Adeyemi. Lagos State High Court, 2022.

Economic and Financial Crimes Commission v. Usman Ibrahim. Federal High Court, Lagos (2021).

Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. Europol Publications (2023).

Fehintola I J, *An Appraisal of the Prospects and Challenges of Cybercrime Investigation and Prosecution in Nigeria*. Master's Thesis, Crescent University, Abeokuta (2023).

Furnell S and Warren M, 'Computer Security, Cybercrime and Cybersecurity: A Comparative Introduction,' *Computers and Security*, (2019) (87) article 101589.

Garner, A. B. *Black's Law Dictionary*. 8th ed., Thomson West, (2009).

Grabosky P, '*Cybercrime: Problems of Classification and Conceptualization,'* Springer, 2016.

Gupta S and Agrawal B, *Cyber Laws: Law Relating to Information Technology, Hacking, Intellectual Property Rights, Trade Marks, E-Commerce, Computers, Computer Software, Internet and Cybercrimes*. Premier Publishing (2009).

Ibikunle F, 'Approach to Cyber Security Issues in Nigeria: Challenges and Solution,' *Department of Electrical & Information Engineering', Covenant University* (2013) (1) (1)

INTERPOL. *Global Cybercrime Trends Report 2023*. INTERPOL Digital Crime Unit, 2023.

Jain A, *Cybercrime: Issues, Threats and Management* (Vol. 1, Isha Books, 1999).

Kolawole A, 'Cybercrime Legislation in Nigeria: Effectiveness and Gaps." ResearchGate, (2022).

Ladan M T, *Cyberlaw and Policy on Information and Communications Technology in Nigeria*. (Ahmadu Bello University Press, 2015).

Laura A, *Cybercrime and National Security: The Role of the Penal and Procedural Law*. (Nigerian Institute of Advanced Legal Studies, 2015).

Makeri Y A, 'Cyber Security Issues in Nigeria and Challenges,' *International Journal of Advanced Research in Computer Science and Software Engineering* (2017) (7) (4).

Muhammed H, 'NCC Clamps Down on Illegal ISPs, Cyber Cafés,' *Daily Trust*, 2 Feb. (2009).

Ngo F T and Jaishankar K, 'Committing Crime in the Digital Age: The Criminological Landscape of Cybercrime,' *International Journal of Cyber Criminology* (2017) (11) (1) .

NIBSS. *Annual Fraud Report*. Nigeria Inter-Bank Settlement System 92024).

Nigeria Police Force – National Cybercrime Centre. **2024**. *Title of Press Release or Report.* Accessed [date]. https://example-source assessed November 2025

Nikhita R G and Ugander G J, 'A Study of Cybersecurity Challenges and Its Emerging Trends on Latest Technologies,' *International Journal of Innovative Science and Research Technology* (2020).

Nojeim G T, 'Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace,' *Statement before the U.S. Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security* (2009) 2 (2).

Nwaobilo I E and Umearokwu UC, 'Cybersecurity as a National Concern: Implications for Nigeria's Digital Economy,' *Nigerian Journal of Information Security Studies* (2024) (3) (1).

Obalola, A. O. and Omotayo, F. A. "Cybersecurity and Legal Framework in Nigeria: Analysis of the Cybercrime Act 2015" (2021). *African Journal of Law & ICT*, 9(2), 45–63.

Obijaka V, 'Legal Framework on Emerging Cybercrimes in Nigeria,' SSRN, 24 Apr. (2024).

Odeh, L. and Alhassan, U. "Reassessing the Effectiveness of the EFCC in Combating Financial Cybercrime in Nigeria" (2020).*Journal of Financial Crime*, 27(4), 1123–1140.

Ogana E, *An Analysis of Legal Framework on Combating Cybercrime in Nigeria*. Master's dissertation, Ahmadu Bello University, Zaria (2017).

Oho S, 'A Critical Analysis of the Cybercrime Law in Nigeria. LL.B thesis, Baze University, Abuja, (2017).

Ojedokun U and Eraye C, 'Socio-economic Lifestyles of Nigerian Cybercriminals,' *International Journal of Cyber Criminology* (2012) (6) (2).

Olanipekun O, 'Cybercrimes in the Banking Sector: Facing the New Wave of Criminals Legally,' *Business Intelligence Journal* (2015)3 (1).

Olateru-Olagbegi O A, 'A Legal Framework for the Restitution of Cyber-Crimes Victims in Nigeria,' *International Journal of Criminal, Common and Statutory Law* (2024) (4) (2)

Olayemi O J, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria,' *International Journal of Sociology and Anthropology* (2014) (6) (3).

Oniye S and Kannike A A, 'Yahoo Plus and Digital Fraud in Nigeria: Socio-cultural Perspectives and Enforcement Challenges,' *KWASU Space Journal of Social and Technological Studies* (2022) (1) (2)

Ortese P T, 'An Appraisal of the Nigerian Cybercrimes Law from Comparative Perspective,' *Benue State University Makurdi Law Journal* (2023) (12) (1).

Osho G S and Olayemi J, 'Cybercrime and Cybersecurity in Nigeria: The Role of Legislation,' *African Journal of Criminology and Justice Studies* (2018) (11) (1).

Pinheiro Legal Practitioners. *Adapting to Change: The Impact and Challenges of Cybercrime in Nigeria and the Way Forward* (2022).

Reddit. 'The Internet Never Forgets,' (Reddit, 2018).

Sahara Reporters. 'ECOWAS Court Declares Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful,' *Sahara Reporters*, 22 Mar. (2023).

Sarker I H and others, 'Machine Learning-Based Cybersecurity Intrusion Detection: A Comprehensive Review,' *Security and Privacy* (2020) (3) (3).

Sarum J, 'Challenges and Solutions of Cybercrimes in Nigeria,' *International Journal of Academia Education* (2022).

Tade O and Adeniyi O, 'Yahoo Boys' and Criminal Entrepreneurship in Nigeria,' *International Journal of Cyber Criminology* (13) (1) (2019).

Umejiaku N O and Anyaegbu M I, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria,' *International Journal of Computers & Technology* (2018) (15) (10).

Wall D S, *Cybercrime: The Transformation of Crime in the Information Age*. (Polity Press, 2007).

World Economic Forum. *Global Risks Report 2024*. (2024)