THE EVOLUTION OF CYBERCRIME IN NIGERIA: EMERGING THREATS, LEGAL GAPS, AND THE DIGITAL FUTURE OF LAW ENFORCEMENT.

BY

Noel Eseose OSUMAH

LAW2002949

A LONG ESSAY WRITTEN AND SUBMITTED TO THE FACULTY OF LAW, UNIVERSITY OF BENIN IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LLB) OF THE UNIVERSITY OF BENIN, BENIN CITY.

NOVEMBER, 2025

CERTIFICATION

I, **Noel Eseose OSUMAH**, with Matriculation Number **LAW2002949**, hereby certify that apart from references to other persons' 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.

_____

Noel Eseose OSUMAH
LAW2002949

APPROVAL

We certify that this project was written and completed by **Noel Eseose OSUMAH**, with Matriculation Number **LAW2002949** in partial fulfillment of the requirement for the award of a bachelor of Laws (LL.B) Degree.

MRS. O. T. OTASOWIE
PROJECT SUPERVISOR _____ **SIGNATURE AND DATE**

DR (MRS) OBIAGELI FRANCISCA OSUJI
PROJECT COORDINATOR _____ **SIGNATURE AND DATE**

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

DEDICATION

I dedicate this research to God Almighty.

ACKNOWLEDGEMENT

I express my profound gratitude to God Almighty, whose grace, wisdom, and strength have guided me throughout the course of this research. His constant help has sustained me from the initial conception of this work to its completion.

My sincere appreciation goes to my supervisor Mrs O. T. Otasowie, whose patience, intellectual guidance, and constructive critiques shaped the direction and quality of this project. I am truly grateful for the time, encouragement, and academic discipline you invested in me.

To my amazing family, most especially Mr & Mrs Osumah, who has been my backbone throughout this journey, thank you for your unwavering love, prayers, and moral support. Your belief in my abilities gave me the confidence to persevere even when the research process became demanding.

I also extend my appreciation to my friends turn family and colleagues who offered insightful discussions, shared materials, and encouraged me during the writing of this project. Their support created an environment of motivation and shared learning.

Finally, I appreciate every author, researcher, and institution whose works and materials enriched the depth of this study. This project is a product of collective knowledge, and I acknowledge that contribution with gratitude.

TABLE OF STATUTES

A. Nigerian Statutes

Advance Fee Fraud and Other Fraud Related Offences Act 2006.

Constitution of the Federal Republic of Nigeria 1999 (as amended).

Criminal Code Act, Cap C38, Laws of the Federation of Nigeria 2004.

Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024).

Economic and Financial Crimes Commission (Establishment) Act 2004 (as amended).

Evidence Act 2011.

Money Laundering (Prevention and Prohibition) Act 2022.

Police Act 2020.

B. Comparative Statutes

Computer Fraud and Abuse Act 1986 (United States).

Computer Misuse Act 1990 (United Kingdom).

Cybersecurity Information Sharing Act 2015 (United States).

Online Safety Act 2023 (United Kingdom).

C. International Instruments

Budapest Convention on Cybercrime 2001 (Council of Europe).

Mutual Legal Assistance Treaties (MLATs).

United Nations Office on Drugs and Crime (UNODC) Model Cybercrime Frameworks.

INTERPOL Cybercrime Collaboration Framework.

TABLE OF CASES

LIST OF ABBREVIATIONS

AGF	Attorney-General of the Federation
CFAA	Computer Fraud and Abuse Act
CISA	Cybersecurity Information Sharing Act
CMA	Computer Misuse Act
CNII	Critical National Information Infrastructure
CPS	Crown Prosecution Service (United Kingdom)
DOJ	Department of Justice (United States)
EFCC	Economic and Financial Crimes Commission
FBI	Federal Bureau of Investigation (United States)
FRN	Federal Republic of Nigeria
ICPC	Independent Corrupt Practices and Other Related Offences Commission
IC3	Internet Crime Complaint Center
LFN	Laws of the Federation of Nigeria
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
NCC	Nigerian Communications Commission
NFIU	Nigerian Financial Intelligence Unit
UNODC	United Nations Office on Drugs and Crime
VPN	Virtual Private Network

TABLE OF CONTENTS

ABSTRACT

This research examines the evolution of cybercrime in Nigeria, highlighting how rapid digitization has created new avenues for offences such as financial fraud, identity theft, ransomware attacks, and cyberstalking. Although Nigeria has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and established specialized institutions for enforcement, the country continues to face persistent challenges in implementation. Weak institutional coordination, inadequate technical capacity, slow investigative procedures, underreporting, and limited public awareness all contribute to the widening gap between law and practice. The study employs a doctrinal research methodology, analyzing statutory provisions, case law, institutional frameworks, and scholarly commentary. It reveals that cybercrime persists not because of a lack of legislation, but because enforcement structures remain fragmented and technologically outdated. Comparative insights from jurisdictions such as the United States and the United Kingdom demonstrate that successful cybercrime control depends on sustained investment in digital forensics, inter-agency collaboration, and public-private partnerships with telecom and fintech sectors.

The study recommends targeted reforms including a comprehensive amendment of the 2015 Act, improved institutional coordination, training of cybersecurity personnel, enhanced digital infrastructure, stricter financial monitoring systems, and greater public digital literacy. It concludes that Nigeria's ability to combat emerging digital threats and protect its socio-economic future depends on building stronger, technology driven, transparent, and independent enforcement institutions.

CHAPTER ONE

GENERAL INTRODUCTION

1.1 INTRODUCTION

The essay appraises the potency of the legal and institutional frameworks for combating cybercrime in Nigeria. With the ever-evolving computer technology, computer-related crime and cybercrime have become a significant global challenge. Cybercrimes are offences that are committed against persons or a group of persons with criminal intents to deliberately harm the reputation of the victim or cause physical or psychological injury or loss, to the victim directly or indirectly, using contemporary telecommunications networks such as internet and mobile phones. In Nigeria, cybercrime is increasing each day as the internet continues to permeate every nook and cranny of our society and no one can predict the next dimension. However, due to the damage and loss suffered by customers and stakeholders causing significant reputation and image problems, many countries are developing strategies to avoid, track and contain cybercrime threats.

In response to the numerous requests and demands from fretful stakeholders in both the Information Communication Technology (ICT) and legal sectors, former President Goodluck Jonathan, in his administration, signed into law the Cybercrime Act on May 15th 2015. The Act became validly enforceable within the provisions of the Nigerian legal system. However, Cybercrime was already widespread before the enactment of the Cybercrimes Act, which was enacted to comprise the growing spate of internet offences by seeking to arrest, punish and sentence any individual guilty of perpetuating cybercrime and other connected offences. The Act has been greatly criticized by some authors as it lacks what it takes to adequately combat the menace. However, the Cybercrime Act is robust but on the other hand, there is a lack of effective enforcement

strategy. Despite the legislation combating cybercrime, it is still prevalent in all parts of Nigeria.

The history of cybercrime concurs with the advancement of the Internet itself. The first crimes were simple hacks but as the Internet became more established so too did the cyber-attacks. While cybercrime existed before this, the first major wave of cybercrime emerged with the widespread use of email in the late 1980s and early 1990s. This development permitted the proliferation of scams such as advance-fee fraud and phishing as well as the distribution of malware directly into users' inboxes. With the development of technology, massive digitalization and unprecedented interconnectivity provided by the internet has been an advantage to different classes of persons, including criminals. Historical antecedent demonstrates that unsanctioned access, damage to property, theft and distribution of offensive and indecent materials are all considered as familiar cybercrimes.

In Nigeria, cybercrimes are executed by individuals, ranging from young to old, but in most instances, youths. Numerous youths indulge in cybercrime activities with the purpose of profit making since the instruments for hacking in modern time have become affordable by many. Nigeria's notoriety in cybercrimes worldwide is an open secret. There is hardly any crime which is not committed on the cyberspace by Nigerians.

Due to this, the Cybercrime Act was sponsored by the Federal Ministry of Justice. The Act is meant to provide an operative and united legal, regulatory and institutional framework for the prevention, detection, prohibition, prosecution and punishment of cybercrimes in Nigeria.

However, despite the Cybercrime Act, the problem of cybercrime is still evident in Nigeria at a great level. This ugly tend acts as a cankerworm against economic

development in Nigeria and has compounded the challenges facing Nigeria against corruption and other vices.

Therefore, this research is to investigate the nature and types of cybercrime in Nigeria, and the effectiveness of the laws available for combating cybercrime in Nigeria.

1.2 BACKGROUND TO THE STUDY

The rise of the internet and digital technology has made cybercrime a pressing legal and security issue worldwide. Nigeria, with its growing online population and e-commerce activities, is particularly vulnerable to crimes such as computer hacking, online fraud, cyberstalking and other forms of digital offense. To address these challenges, the Nigerian government enacted the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015**,** a statute designed to provide an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria[1]. In fact, the Act explicitly codifies a wide range of offenses, for example, Section 6 criminalizes unauthorized computer access, unlawful access to a computer, Section 13 outlaws computer related forgery, Section 14 penalizes computer related fraud, Section 24 prohibits certain messages sent via computer like cyberstalking and related abuses and Section 25 addresses cybersquatting, among others. By 2024 the law was further amended, reflecting ongoing legislative attention to digital crime[2]. Importantly, the Act also confers broad jurisdiction to Nigerian courts: for instance, Section 50 grants the Federal High Court authority to try cyber offenses committed even outside the country, giving the law extraterritorial reach. Thus, Nigeria's

---

1 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ICT Policy Africa, *'Nigeria: Cybercrimes (Prohibition, Prevention, etc.) Act, 2015'* (2015) <https://ictpolicyafrica.org/fr/document/h52z5b28pjr?page=2> accessed 22 August 2025.

2 ICLG, *'*Cybersecurity Laws and Regulations — Nigeria Chapter*'* (11 June 2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria#:~:text=1,Amendment%20Act,%202024> accessed 24 August 2025.

Cybercrimes Act (2015, as amended) represents a far reaching effort to adapt national law to modern technological realities and to deter internet enabled crime.

Despite its comprehensive scope, the Cybercrimes Act's enforcement raises numerous issues. Several sections of the Act have been the subject of court scrutiny. For example, the constitutionality of Section 24(1) which proscribes the sending of grossly offensive or false messages for purposes of causing "annoyance, inconvenience or needless anxiety" was challenged in *Okedara v Attorney General of the Federation*[3]. The Court of Appeal in Lagos dismissed that challenge, holding that Section 24(1) was neither vague nor inconsistent with fundamental rights. This illustrates how the law's broad provisions can implicate free expression rights under the 1999 Constitution, and how courts are working to interpret the Act's language. In another illustration, the *Julius v. FRN* appeal involved multiple counts under the Cybercrimes Act, the appellant was charged with unlawful access, computer related forgery , fraud , cyberstalking, cybersquatting, and even racist speech offenses [4]. These cases show that Nigeria's cybercrime law is already being tested across a spectrum of activities, and that its interpretation by the courts will shape the practical boundaries of what behavior is punishable.

Nigeria does not rely solely on the Cybercrimes Act for cyber related offenses. Other federal statutes complement it. For instance, the Advance Fee Fraud and other Related Offences Act, 2006[5], targets a common form of online fraud, and economic and financial crimes laws such as the Economic and Financial Crimes Commission (Establishment) Act[6], which was originally enacted in 2002, and later repealed and re-enacted in 2004, and Money Laundering Act,2022[7], are often used against perpetrators of high tech scams.

---

3 (2018) LPELR-45183 (CA).
4 (2021) LPELR-54201 CA.
5 Advance Fee Fraud and Other Fraud Related Offences Act 2006, LFN 2006.
6 Economic and Financial Crimes Commission (Establishment) Act 2004, LFN 2004.
7 Money Laundering (Prevention and Prohibition) Act 2022, Laws of the Federation of Nigeria

Together, these laws form a network of primary legal tools aimed at curbing technological abuses.

In summary, the background to this study lies in the intersection of growing cyber threats in Nigeria and the country's evolving legal response. The Cybercrimes Act of 2015 (and its 2024 amendment) is at the center of this framework, defining a range of digital offenses and conferring special jurisdictional powers. It interacts with constitutional rights notably free expression and with other criminal statutes. As the Act is applied in courts, new legal interpretations emerge. Understanding this context is essential for appreciating the problems, objectives, and questions set out below.

1.3 STATEMENT OF PROBLEM

Nigeria is the fifth jurisdiction after Russia, Ukraine, China and United States of America, where the world records the highest number of cybercrimes.[8] Thus, legislatures have been struggling to redefine and restructure laws that fit into crimes done by cyber culprits in the cyber space. Some of these problems are:

i. Evolution and Forms of Cybercrime in Nigeria: Cybercrime in Nigeria keeps growing despite the Cybercrimes Act 2015. Among young people, it has become a widespread practice driven by unemployment, peer pressure, and the lure of quick wealth. This raises the question of how cybercrime has evolved and what forms are now most common.

ii. Effectiveness of the Cybercrimes Act 2015: The Act was meant to curb cyber offences, yet many of its provisions are unclear and outdated. These gaps limit its ability to address modern cyber threats, calling into question how effective the law truly is.

iii. Institutional and Enforcement Challenges: Agencies like the EFCC and the Nigeria Police Force still lack adequate tools, training, and forensic expertise. These weaknesses

---

[8] Nairametrics, 'Nigeria ranks 5th in global cybercrime index' https://nairametrics.com/2024/04/12/nigeria-ranks-5th-in-global-cybercrime-index accessed 26 August 2025.

make investigation and prosecution difficult, showing the institutional barriers to enforcement.

iv. Impact of Emerging Technologies: New technologies such as social media, crypto-currency, and artificial intelligence have made cybercrime more complex. Law enforcement struggles to keep up, prompting concern over how these tools shape both cyber offences and responses.

v. Evidential and Legal Reform Issues: Prosecutors face major hurdles with electronic evidence. Collecting, preserving, and proving digital data under the Evidence Act remains highly technical. This highlights the need for stronger reforms to make cybercrime laws more effective.

1.4 AIM AND OBJECTIVES OF THE STUDY

The aim of this essay is to examine the legal framework for combating cybercrime in Nigeria.

Its objectives are:

i. To access the legal regime for combating cybercrime in Nigeria
ii. To examine the challenges for facing the enforcement of cybercrime law in Nigeria
iii. To compare the laws regulating cybercrime in Nigeria to other jurisdictions
iv. To identify the essential reforms required to fortify the legal framework to regulate cybercrime in Nigeria.

1.5 RESEARCH QUESTIONS

To guide this study, the following research questions are posed:

i. How has cybercrime evolved in Nigeria, and what are the predominant forms today?
ii. To what extent does the Cybercrimes Act 2015 address contemporary cyber threats?
iii. What institutional and judicial challenges affect the enforcement of cybercrime laws in Nigeria?

iv. How do emerging technologies and digital platforms influence the nature of cybercrime and law enforcement responses?
v. What reforms or strategies could strengthen Nigeria's legal and institutional response to cybercrime?

These questions are designed to ensure a thorough examination of both the statutory text and its real world application.

1.6 SIGNIFICANCE OF THE STUDY

This study is significant because it addresses the emerging and complex problem of cybercrime in Nigeria from multiple perspectives academic, legal, institutional, and societal. Academically, it fills a gap in scholarship by examining the evolution of cybercrime and its legal regulation. Legally, it critically evaluates the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and related statutes, highlighting gaps, enforcement challenges, and the need for alignment with international standards. Institutionally, the study provides practical insights for law enforcement agencies, recommending capacity building, technological upgrades, and improved investigative frameworks. Socially, it emphasizes protecting citizens' rights, enhancing trust in digital platforms, and strengthening national cybersecurity. Ultimately, the research contributes to shaping a secure, technologically resilient, and rights respecting digital environment in Nigeria.

1.7 SCOPE AND LIMITATION

The essay is an examination of the legal framework on cybercrime. It would put into consideration the concept of cybercrime, placing importance on the adequacy of the legal framework combating cybercrime. However, this study shall be limited to Nigeria but instances shall be made from other jurisdictions.

1.8 METHODOLOGY

The essay will adopt intended method for this research is qualitative essay and not measurement that is estimated by quantity. The major substantiated/supported evidence accepted by most authorities that would be employed is journal, articles textbooks and legislations. The effectiveness of the current legal framework on cybercrime in Nigeria would be ascertained. Recommendations and solutions to identified problems and loopholes will be proposed.

CHAPTER TWO

CONCEPTUAL CLARIFICATION, THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 INTODUCTION

Cybercrime has become a major global concern, with Nigeria experiencing its share of the problem as technology and internet use expand. The country's growing digital landscape has brought both progress and vulnerability, exposing individuals, businesses, and government institutions to crimes such as hacking, online fraud, identity theft, and cyberstalking. This chapter lays the foundation for understanding cybercrime within Nigeria's legal and social context. It clarifies key concepts and applies relevant criminological theories such as routine activity, deterrence, to explain the motivations behind cyber-offences.

It also reviews existing literature to trace the development, causes, and effects of cybercrime, as well as the challenges confronting law enforcement and legal institutions. By identifying gaps in current responses, the chapter provides the framework for the deeper analysis that follows in subsequent chapters.

2.2 Cybercrime

In simple terms, cybercrime refers to any unlawful act committed using or against computer systems, networks, or data. It includes offences such as hacking, online fraud, phishing, identity theft, and cyberstalking. According to Encyclopaedia Britannica, cybercrime is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing

identities, or violating privacy.[9] This definition shows that computers and the internet can serve not only as tools but also as targets of crime. Similarly, researchers at the University of Groningen describe cybercrime as behaviour wherein a technological device is the primary means, and the offender's aim is to access information or exploit the internet for malicious purposes.[10]

Despite these attempts, the United Nations Office on Drugs and Crime (UNODC) notes that there is no single universally accepted definition of cybercrime. The UNODC defines it broadly as an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, or to affect individuals.[11] The organization further explains that cybercrime can be divided into two main categories: cyber-dependent crimes, which can only be committed using ICT for example, hacking or malware attacks, and cyber-enabled crimes, which are traditional crimes such as fraud or harassment that have been expanded by the use of digital technology.[12] A similar classification appears under the Council of Europe's Convention on Cybercrime, often called the Budapest Convention. It defines cybercrime as offences against and by means of computer systems[13]. The Convention lists several key offences, including illegal access, data interference, system interference, misuse of devices, and computer-related fraud. By focusing on threats to the confidentiality, integrity, and

---

9 Encyclopaedia Britannica, "Cybercrime," <https://www.britannica.com/topic/cybercrime> accessed 23 September 2025

10 University of Groningen, Cybercrime and Illicit Trade <https://www.rug.nl/rudolf-agricola-school/research/development-security-and-justice/cybercrime-illicit-trade.pdf> accessed 23 September 2025

11 United Nations Office on Drugs and Crime (UNODC), Cybercrime in Brief, <https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html> accessed 23 September 2025

12 Ibid.

13 Council of Europe, 'Convention on Cybercrime (Budapest Convention)' <https://www.coe.int/en/web/cybercrime> accessed September 2025

availability of computer data and systems, the Budapest Convention provides a global framework for countries including Nigeria to model their domestic cybercrime laws.

The European Commission also offers a clear and inclusive definition, describing cybercrime as criminal acts committed online by using electronic communications networks and information systems.[14] This view covers a wide range of online misconduct, from attacks against information systems to identity theft, online scams, and the distribution of illegal digital content. From these different perspectives, certain common features can be identified. First, cybercrime always involves a connection between illegality and technology either through the use of ICT as a tool for committing offences or as the direct target of those offences. Second, cybercrime is inherently transnational, often crossing national borders and complicating issues of jurisdiction and law enforcement. Third, experts agree that cybercrime has a dual nature: while some crimes depend entirely on technology, others merely use it as a modern means of execution.

Based on these shared principles, cybercrime may be defined as:

> Any conduct that constitutes an offence under domestic or international law, committed by, through, or against an information and communication technology system or data, where such system or data plays a central role in the commission, facilitation, or outcome of the offence.

This definition brings together both the legal and technological elements of cybercrime. It aligns with the UNODC's recognition of cyber-dependent and cyber-enabled offences, while also reflecting the Budapest Convention's focus on protecting the integrity of information systems.

In conclusion, cybercrime is not merely a technical issue but a profound legal and social challenge that evolves alongside technology. While different institutions define it in slightly different ways, they all agree on its essence,the misuse of digital technology for

---

[14] European Commission, 'Cybercrime Policy Overview' <https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en> accessed 23 September 2025

unlawful purposes. Frameworks such as the UNODC's approach, the Budapest Convention, and the European Commission's policies provide a strong foundation for national laws like Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act of 2015. To combat this global threat effectively, nations must continue refining their definitions and laws, ensuring they remain adaptable to the ever-changing realities of cyberspace.

2.3 Types of Cybercrime in Nigeria

Cybercrimes are criminal acts that are carried out via the use of computer or automated devices or internet. There are various Cybercrimes common in Nigeria, such as;

2.3.1 Advance Fee Fraud

Advance Fee Fraud, popularly called "419", remains one of the most persistent and damaging cybercrimes in Nigeria today. It operates on a simple but devastating deception convincing unsuspecting victims to pay a sum of money upfront, often disguised as processing fees, investment deposits, or clearance costs, with the false promise of receiving a much larger financial reward later. Once the payment is made, the fraudsters disappear, leaving victims in financial distress.[15]

Nigerian law takes a firm stance against this offence through Section 419 of the Criminal Code, the Advance Fee Fraud and Other Fraud-Related Offences Act 2006, and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. These laws collectively criminalize obtaining money by false pretence, internet fraud, and related offences that have evolved in the digital age. Today's 419 scams are no longer confined to letters or faxes, they thrive through social media impersonations, fake online investments, romance scams, and counterfeit business proposals.

---

[15] Solomon Gwom, 'A Focus on Advanced Fee Fraud in Nigeria: Nature, Prevalence and the Urgent Need for Enforcement of Relevant Laws' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421734> accessed 23 september 2025.

A notable example occurred in April 2025, when the Oyo State High Court in Ibadan convicted Olaniyan Gbenga Amos for operating an online investment fraud through Detorrid Heritage Investment Limited. He was found guilty of obtaining money by false pretence and was sentenced to 63 years imprisonment.[16] Similarly, in May 2025, the Federal High Court in Port Harcourt sentenced three men, Rex Akah Kinikachi Kelvin, Kennedy Chinedu Eleyi-Waltar, and Chris Orji to 90 months imprisonment each for impersonation and online fraud via Telegram, with their gadgets and a vehicle forfeited to the government.[17]

These cases highlight the growing determination of Nigerian courts to combat cyber-enabled advance-fee fraud. Through firm sentencing and asset forfeiture, the judiciary continues to send a clear message that digital deception, no matter how sophisticated, will not go unpunished.

2.3.2 Dating Scam

Dating scams, also referred to as romance fraud or love scams, constitute a prominent form of cybercrime in Nigeria. Dating or romance scams are a form of cyber-fraud where the perpetrator fabricates a romantic or emotional online relationship in order to deceive the victim into sending money or divulging sensitive personal data. The goal is financial gain, often under false pretences such as emergencies, travel costs, or investment opportunity. In many instances, the scammer poses as a foreigner, military officer, businessperson, or someone in distress to gain trust and legitimacy.

---

16 The Guardian Nigeria, 'Serial investment fraudster bags 63 years in Ibadan' (2025) <https://guardian.ng/news/nigeria/metro/serial-investment-fraudster-bags-63-years-in-ibadan/> accessed 23 September 2025.

17 The Guardian Nigeria, 'Three convicted of Internet fraud sentenced to 90 months imprisonment' (2025) <https://guardian.ng/news/nigeria/metro/three-convicted-of-internet-fraud-sentenced-to-90-months-imprisonment/ accessed 23 September 2025.

In Nigeria, the legal foundation for prosecuting such scams is principally the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (as amended). Section 22 of that Act addresses identity theft and impersonation. A person who fraudulently impersonates another, living or dead, with intent to gain advantage, obtain property, or cause disadvantage in another, is liable on conviction to imprisonment for up to seven years or a fine of not more than ₦5,000,000, or both.[18] This provision is often invoked in romance scam prosecutions, where the offender pretends to be someone else to induce confidence in the victim.

There are verified Nigerian cases confirming that courts do convict for dating scams. In 2025, the EFCC announced that a Lagos court sentenced a man to two years imprisonment after he confessed that he had engaged in a dating scam and benefited ₦200,000 from it.[19] In another case, the EFCC secured a conviction of one year for an internet fraud offence in Lagos, which the complainant and reports frame as including romantic or dating deception.[20] Earlier, in 2023, the EFCC prosecuted Wano Abdullahi Ahmed for possessing fraudulent documents used in a romance scam: he was found guilty and sentenced to one year's imprisonment for representing himself falsely as "Rita John, a female American." [21] That case demonstrates how falsified identities or documents are used in court to show the deception element necessary for fraud. These cases establish that Nigerian courts do treat romance scams seriously, applying

---

[18] Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, Section 22

[19] EFCC, 'Court Jails Man Two Years for Cybercrime in Lagos' (2025) <https://www.efcc.gov.ng/efcc/news-and-information/news-release/11271-court-jails-man-two-years-for-cybercrime-in-lagos> accessed 29 September 2025.

[20] EFCC, 'Court Jails Man One Year for Internet Fraud in Lagos' (2025) <https://www.efcc.gov.ng/efcc/news-and-information/news-release/11079-court-jails-man-one-year-for-internet-fraud-in-lagos> accessed 29 September 2025.

[21] EFCC, 'Court Jails Man One Year for Possession of Fraudulent Documents in Lagos' (2023) <https://www.efcc.gov.ng/efcc/news-and-information/news-release/9100-court-jails-man-one-year-for-possession-of-fraudulent-documents-in-lagos> accessed 29 September 2025.

cybercrime and related statutes. The consistent use of Section 22 and related provisions underscores that impersonation is central to proving the offence. Also, the practice of forfeiting devices, seizing phones, and examining digital evidence is common in EFCC proceedings.

However, challenges persist. Many romance scams are transnational, victims and perpetrators are in different jurisdictions, complicating evidence gathering and extradition. Digital evidence like chat logs, emails, financial transfers through mules or crypto wallets may be deleted or routed through multiple countries. Identifying the masterminds behind local mules is often difficult. Also, securing restitution for victims is frequently unsuccessful once money has been dispersed or laundered.

In summary, dating scams in Nigeria are not speculative, they are adjudicated, prosecuted, and punished under existing cyberlaws. Known court decisions support the legal theory that impersonation via Section 22 of the Cybercrimes Act and fraud be prosecuted, and devices used are seized as evidence.

2.3.3 Phishing

Phishing is one of the most common and deceptive forms of cybercrime. It occurs when a criminal poses as a trusted institution such as a bank, government agency, or well known business to deceive individuals into revealing confidential information like passwords, credit card numbers, or bank details.[22] The scammer usually contacts the victim through fake emails, text messages, or instant chats that appear legitimate. In many cases, they create counterfeit websites that look identical to real ones, tricking unsuspecting users into entering personal data or clicking malicious links that install harmful software.[23] In

---

[22] NI Ashiru, 'Identifying Phishing as a Form of Cybercrime in Nigeria' <https://www.ajol.info/index.php/naujilj/article/download/215400/203155> accessed 29 October 2025.

[23] LawPedia, 'Identifying Phishing as a Form of Cybercrime in Nigeria' (2025) <https://www.lawpedia.com.ng/identifying-phishing-as-a-form-of-cybercrime-in-nigeria/> accessed 29 October 2025.

Nigeria, phishing is specifically recognized and criminalized under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Section 32(1) of the Act provides that any person who knowingly or intentionally engages in computer phishing shall be liable on conviction to three years imprisonment or a fine of one million naira or both.[24] The Act further defines phishing in Section 58 as the criminal and fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.[25]

Over the past decade, phishing attacks have become a growing threat to Nigeria's digital economy. With the rapid expansion of online banking, mobile payments, and e-commerce, cybercriminals have found fertile ground to exploit unsuspecting users. The National Information Technology Development Agency (NITDA) has issued several warnings to the public, highlighting new phishing techniques that rely on Telegram bots, spoofed Google Forms, and other automated tools to harvest data from users.[26] These evolving tactics reflect the sophistication and adaptability of modern cybercriminal networks.

From a policy standpoint, the inclusion of phishing in the Cybercrimes Act underscores Nigeria's effort to strengthen its legal defences against digital deception. The provision serves not only as a deterrent but also as an empowerment tool for law enforcement agencies such as the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF), who are tasked with investigating and prosecuting such offences. By defining phishing explicitly, the law sends a clear message that cyber fraud is not a minor inconvenience it is a serious criminal act punishable by law.

---

24 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 32(1).

25 Ibid., s 58.

26 Voice of Nigeria, 'NITDA cautions Nigerians against new Cyber attack strategy' (2025) <https://von.gov.ng/nitda-cautions-nigerians-against-new-cyberattack-strategy/ accessed 29 October 2025.

Nonetheless, Nigeria continues to face challenges in fully combating phishing crimes. The rapid evolution of digital tools makes it difficult for legislation and enforcement to keep pace. Moreover, limited technical capacity, inadequate cyber literacy, and low rates of prosecution hinder the effectiveness of the current legal framework. While the Cybercrimes Act provides a strong foundation, there is a pressing need for continued public education, enhanced law enforcement training, and inter-agency collaboration to reduce the prevalence of phishing and other online scams.

2.3.4 Malware

Malware which is short for malicious software refers to any software intentionally designed to perform harmful actions on a computer system, network, or device. This includes viruses, worms, Trojans, ransomware, spyware, rootkits, and other malicious code that can steal data, damage files, exfiltrate information, or deny access to legitimate users. For example, in the Cybersecurity Laws and Regulations Report: Nigeria, it is noted that under Section 32 of the Cybercrimes Act, it is an offence for any person to maliciously cause the spread of viruses or malware that damage computer systems.[27] Malware may be introduced via phishing emails, malicious attachments, drive-by downloads, exploit kits, or through social engineering that lures users to install or run compromised programs.

In Nigeria, the principal law addressing malware is the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 and its amendments. Section 8 criminalizes intentionally or fraudulently hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data acts typical of

[27] Cybersecurity Laws and Regulations Report: Nigeria, ICLG – Nigeria, on Section 32 (spread of viruses/malware) and related provisions, <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria> accessed 29 September 2025.

malware operations.[28] Likewise, Section 28 prohibits the manufacture, importation, distribution or possession of devices or programs including malware designed to commit offences under the Act.[29] The 2024 amendment to the Act tightened these provisions, expanding the scope of unauthorized or fraudulent access and damage involving computer systems.[30] Thus, under Nigeria's cyber-law framework, deploying malware to damage systems or to fraudulently access data is clearly prohibited and may attract criminal sanction.

One real case illustrating malware activity is the U.S. Department of Justice's indictment of a malware-as-a-service network, which included a Nigerian national. In February 2024, authorities announced the dismantling of an international malware operation that sold and distributed malware, and indicted Prince Onyeoziri Odinakachi of Nigeria for conspiracy to commit computer intrusion offences, including causing unauthorized damage to protected computers.[31] This case shows that Nigeria nationals have been held accountable internationally for malware based offences. On the domestic front, while publicized Nigerian court judgments specifically labelled malware cases are rarer, the prevalence of Nigerian hacker groups using malware tools is documented in cyber-security intelligence. The notorious Nigerian BEC (business email compromise) syndicate SilverTerrier has been observed using malware tools like, remote access Trojans to facilitate email compromise and credential theft.[32] In Nigeria, police and cybercrime units frequently

---

28 Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, Section 8

29 Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, Section 28

30 Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024, which broadens scope of unauthorized access/damage, <https://placng.org/i/wp-content/uploads/2024/05/Cybercrimes-Prohibition-Prevention-etc-Amendment-Act-2024.pdf> accessed 29 September 2025.

31 U.S. Department of Justice press release, 'International Cybercrime Malware Service Dismantled… Nigerian National Indicted' (2024) <https://www.justice.gov/archives/opa/pr/international-cybercrime-malware-service-dismantled-federal-authorities-key-malware-sales> accessed 29 September 2025.

32 Wikipedia, 'SilverTerrier (cybercrime syndicate) (documenting malware use by Nigerian BEC groups)' <https://en.wikipedia.org/wiki/SilverTerrier> accessed 29 September 2025.

target suspects in malware-assisted cyber fraud during coordinated operations, seizing computers, storage media, and malicious software as part of digital evidence.

The legal challenges in prosecuting malware offences are substantial. First, attribution is difficult, malware authors often hide behind intermediary servers, proxy chains, or compromised machines. Second, evidence of malware execution like logs, memory dumps may be volatile and erased once discovered, making forensic recovery complex. Third, cross-border jurisdictional issues arise when malware infects systems beyond Nigeria and criminal servers are hosted abroad. Moreover, the pace of malware evolution polymorphic code, zero-day exploits outpaces law enforcement capability in many jurisdictions. Nigeria's recent amendment of its Cybercrimes Act attempts to keep pace by widening definitions of unauthorized access and damage, but enforcement capacity such as technical expertise, coordination with global agencies remains a bottleneck.[33]

2.3.5 Spam

Unsolicited bulk electronic messaging commonly called spam refers to the mass distribution of unwanted commercial or other messages via email, SMS, social platforms or other electronic channels. Spam is often an entry vector for more serious harms including phishing, malware distribution, advance-fee and investment scams because it allows criminals to reach large numbers of potential victims cheaply and anonymously. Cybersecurity and consumer authorities in the United States and Europe characterize spam as unsolicited commercial email or bulk messaging that can facilitate fraud, identity theft and malware infection.[34]

---

[33] Babafemi Tomilehim, 'An Appraisal of the Legal Framework of Cybercrime in Nigeria' <https://www.clrwc.com/2022/04/an-appraisal-of-the-legal-framework-of-cybercrime-in-nigeria?utm_source=chatgpt.com> accessed 29th September 2025.

[34] CISA, 'Recognizing and Avoiding Email Scams (fact sheet)' <https://www.cisa.gov/sites/default/files/publications/emailscams_0905.pdf> accessed 30 September 2025.

Nigeria's principal statute for electronic offences expressly recognizes and criminalizes spamming. The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, Section 32(2) specifically criminalizes spamming carried out with intent to disrupt operations of a computer including public, private or financial institutions and prescribes penalties up to three years' imprisonment, a fine of ₦1,000,000, or both. This statutory placement shows that Nigerian legislators regard spamming not merely as nuisance conduct but as an offence that can threaten system availability and facilitate fraud.[35]

In practice, public EFCC press releases and court reports more commonly record convictions for internet fraud, impersonation, possession of fraudulent documents, or advance-fee offences rather than standalone spamming prosecutions. EFCC news items routinely announce convictions and custodial sentences for internet-enabled fraud, but they typically describe the offence in terms of fraud and impersonation rather than labeling it spam. This suggests that while the Act criminalizes spamming, prosecutors usually charge the fraudulent or deceptive outcome such as obtaining money or property by false pretence, impersonation rather than the form of bulk messaging alone.[36]

There are, however, clear international precedents showing that mass unsolicited messaging can attract severe criminal sanctions when it is used to commit or facilitate crime. For example, in the United States, Sanford Wallace widely publicized as the "Spam King" pleaded guilty to sending millions of unsolicited messages and disobeying court orders, and received imprisonment and restitution orders; U.S. authorities have used both criminal and civil remedies against prolific spammers. That international practice

---

35 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, Section 32

36 EFCC, 'Court Jails Man One Year for Internet Fraud in Lagos' (2025) <https://www.efcc.gov.ng/efcc/news-and-information/news-release/11079-court-jails-man-one-year-for-internet-fraud-in-lagos> accessed 30 September 2025.

reinforces Nigeria's statutory approach of treating spamming as an enabler of more serious cybercrime.[37]

From a prosecutorial and policy perspective, spamming raises familiar challenges, senders use botnets/proxies, logs, and jurisdiction (spam campaigns and servers are often cross-border). Nigeria's Section 32 on spamming combined with EFCC's active anti-internet fraud operations provides legal tools to pursue actors who use bulk messaging to perpetrate fraud; nonetheless, publicly reported judgments labeled strictly as spam are uncommon, prosecutions tend to focus on the fraudulent result like the money obtained and related offences. Strengthening technical forensic capacity and international mutual assistance remain critical priorities to make Section 32 practically effective.[38]

2.3.6 Wiretapping/Illegal Interception of Telecommunication

Illegal interception of telecommunications, also known as wiretapping or unauthorized surveillance of private communications, refers to any act of covertly monitoring or recording phone calls, messages, or data transmissions without the consent of at least one party, or without lawful authority. The rights to privacy and confidentiality of communications are protected under Section 37 of the Constitution of Nigeria, which guarantees the privacy of correspondence, telephone conversations and telegraphic communications. Any interception without lawful authority or judicial warrant is generally unlawful and may infringe constitutional and statutory rights.[39]

---

37 U.S. Department of Justice, Sanford 'Spam King Wallace Pleads Guilty to Spamming Facebook Users' (2015) <https://www.justice.gov/usao-ndca/pr/sanford-spam-king-wallace-pleads-guilty-spamming-facebook-users-and-disobeying-court-order> accessed 30 September 2025.

38 UNODC, 'Global Cybercrime Report: The Challenge of Cross-Border Spam and Botnets' <https://www.unodc.org/> accessed 30 September 2025.

39 VC Ikpeze and CA Aniekwe, 'Unauthorized Wiretapping of Private Telephone Communications: Appraising the Legal Framework for the Protection of Rights to Privacy in Nigeria'. <https://www.nigerianjournalsonline.com/index.php/LASJURE/article/view/.com> accessed 30 September 2025

Under the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, there are clear provisions dealing with interception. Section 39 provides for interception of communications in certain circumstances with lawful authority.[40] Conversely, Section 12 of the Act criminalizes unlawful interception: it states that any person who intentionally and without authorization intercepts non-public transmissions of computer data, or content, or traffic data, including electronic signals or communications, is guilty of an offence. Penalties include fines, imprisonment, or both.[41]

There have been public instances and controversies in Nigeria concerning wiretapping or interception, though confirmed court decisions are fewer. In 2021, the Minister of Communications and Digital Economy, Prof. Isa Pantami, disclosed that the 2015 Cybercrime Act allows lawful interception of phone conversations by government agencies, subject to legal requirements. This statement confirms that interception is not per se illegal when properly authorized.[42] A significant recent case involving privacy right concerns is *Ezugwu vs MTN*. In 2025, the Court of Appeal fined MTN Nigeria N15 million for sending unsolicited messages to its subscribers, a decision that intersects with privacy and unsolicited communications, which are related to notions of unlawful access or interception of communications like spam or unsolicited messages though not exactly classic wiretapping. This case demonstrates that telecommunications companies can be held liable for violating customers' rights to quiet and private enjoyment of their telecommunication services.[43]

---

40 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, Section 39.

41 Cybercrime Act Does Not Create an Enforcement Agency (24 May 2016), discussing Section 12 and interception under Nigerian law. <https://www.thisdaylive.com/2016/05/24/cybercrime-act-does-not-create-an-enforcement-agency/> accessed 30 September 2025.

42 Pantami: Cybercrime Act Allows Lawful Interception of Phone Conversations, PRNigeria (2021) <https://prnigeria.com/2021/09/07/cybercrime-act-phone-pantami/> accessed 30 September 2025

43 *Ezugwu Emmanuel Anene v. MTN Nigeria Communications Ltd* (Court of Appeal, Abuja Division, 20 December 2024, unreported) <https://guardian.ng/news/unsolicited-messagestime-to-strengthen-consumer-privacy-rights/> accessed 30 September 2025.

Key legal challenges in wiretapping interception cases include: determining lawful vs unlawful interception (obtaining court-ordered warrants vs arbitrary surveillance), preservation of communications data, chain of custody of intercepted communications for admissibility, balancing national security or law enforcement interests with privacy and human rights, and ensuring oversight of security agencies.

2.3.7 Password Sniffing

Password sniffing often referred to as packet sniffing is the process of intercepting and capturing data packets moving across a network to retrieve sensitive credentials such as usernames and passwords. Attackers deploy packet-capture tools like Wireshark or tcpdump, often on unsecured Wi-Fi networks or compromised servers, to extract authentication details transmitted in plain text. In practice, password sniffing is a subset of network eavesdropping, and it poses severe risks because many users reuse credentials across multiple platforms, amplifying the harm caused when a single password is compromised.[44] Under Nigerian law, password sniffing falls squarely within the prohibitions of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015. Section 6 criminalizes unauthorized access to computer systems and networks, covering scenarios where sniffed passwords are used to break into accounts. Section 12 criminalizes unlawful interception of non-public transmissions, which includes sniffing credentials during network transit. Together, these sections provide a comprehensive statutory basis for prosecuting password sniffing. The Cybercrimes (Amendment) Act 2024 strengthened these provisions by broadening unauthorized access to include possession or trafficking of stolen credentials and empowering enforcement agencies like the EFCC

[44] Ryan Clancy, 'Password Sniffing in Ethical Hacking and Its Types Explained' <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hacking-password-sniffing/> accessed 30 September 2025.

and NG-CERT to demand data retention for forensic investigations.[45] The Economic and Financial Crimes Commission (EFCC) has prosecuted numerous cyber-fraud cases in which stolen credentials played a central role. For instance, EFCC press releases frequently report convictions of fraudsters found with multiple stolen ATM card details, email logins, or access credentials harvested from phishing and sniffing activities.[46] Although not always framed in technical terms, these prosecutions fall under the statutory provisions on unauthorized access and password misuse. In practice, courts rely on forensic evidence extracted from seized devices and network logs to establish liability. International jurisprudence also offers useful parallels. In the United States, *United States v. Albert Gonzalez* saw the conviction of hackers who used packet sniffers to steal millions of credit card details, resulting in sentences of up to 20 years' imprisonment.[47] Similarly, in the *Google Street View* litigation, courts addressed whether the interception of unencrypted Wi-Fi packets amounted to unlawful wiretapping, underscoring the legal complexity of password sniffing and network interception.[48] These cases demonstrate that password sniffing is globally treated as a serious cybercrime, punishable with heavy sanctions, and provide interpretative guidance for Nigerian courts as local jurisprudence develops. From a preventive perspective, addressing password sniffing in Nigeria requires a blend of legal enforcement and technological safeguards. Statutorily, rigorous application of Sections 6 and 12 of the Cybercrimes Act is essential to deter offenders. Technically, Nigerian institutions must mandate encryption standards across all networks

---

45 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria), ss. 6, 8, 12.

46 Premium Times, 'EFCC Traces $30,000 to Suspected Internet Fraudster' <https://www.premiumtimesng.com/news/more-news/792585-efcc-traces-30000-to-suspected-internet-fraudster.html> accessed 30 September 2025.

47 *United States v. Albert Gonzalez*, 132 F.3d 41 (9th Cir. 1997) <https://www.justice.gov/archives/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail> accessed 30 September 2025.

48 *Joffe v. Google*, 729 F.3d 1262 (9th Cir. 2013) <https://www.wired.com/2011/06/google-wiretap-breach> accessed 30 September 2025.

and promote multi-factor authentication to render sniffed passwords less useful.[49] These measures, combined with judicial awareness of international precedents, will strengthen Nigeria's ability to respond effectively to password sniffing as part of the wider cybercrime threat landscape.

2.3.8 Cyberstalking

Cyberstalking is a modern form of harassment using digital platforms, where an offender persistently uses electronic communications such as messages, emails, social media posts to threaten, intimidate, harass, or cause fear in a victim. The behavior often involves repetitive messaging, spreading false accusations, monitoring, and other intrusive acts. In Nigeria, the statutory basis for prosecuting cyberstalking lies primarily in Section 24 of the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, as amended. Under Section 24(1) of the 2015 Act, a person who knowingly or intentionally sends a message or other matter via computer system or network that is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes such a matter to be sent, or sends a false message with the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, intimidation, enmity, hatred, ill will, or needless anxiety, commits an offence. The penalty is a fine of up to ₦7,000,000 or imprisonment for up to three years, or both.[50] Beyond subsection (1), Section 24(2) expands the offence to more serious conduct: sending messages with intent to bully, threaten, harass another person in a way that places them in fear of bodily harm or death, or containing threats to kidnap, harm property or reputation, or extort money. Convictions under (2) may attract

---

[49] Paul Ohkum, 'Legal Issues Surrounding Monitoring During Network Research' <https://conferences.sigcomm.org/imc/2007/papers/imc152.pdf?utm_m> accessed 30 September 2025.

[50] Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, s. 24(1)

much heavier penalties, including up to ten years' imprisonment and fines up to ₦25,000,000 depending on the nature of threats or extortion involved.[51]

One confirmed judicial development is the decision in *Okedara v. Attorney General* , where the court upheld the constitutionality of Section 24(1) against a challenge that it violated freedom of expression under Section 39 of the 1999 Constitution. The Court found that the language of subsection (1) is clear, and that the law's restrictions on speech fall within the permissible exceptions under Section 45 of the Constitution.[52] This case is especially important because it is a direct courtroom affirmation of Section 24's validity in Nigeria.

However, there are several reported prosecutions in the media under Section 24. For example, in 2023–2024, journalists and bloggers were charged with cyberstalking and defamation for social media posts critical of public figures, e.g. the founder of Naija Live TV was reported to have faced cyberstalking accusations under Section 24 plus defamation charges; similarly, arrests of media personnel on cyberstalking charges have been documented in press reports.[53] These cases show that Section 24 is being invoked in practice, often in politically sensitive contexts.

A major legal controversy is the decision of the ECOWAS Court of Justice (2022) which found that Section 24(1) as originally enacted violated rights to freedom of expression under regional human rights instruments like the African Charter, International Covenant on Civil and Political Rights (ICCPR) because of its vagueness and arbitrary application.

---

51 Legal Implications of Cyber-Bullying and Online Harassment in Nigeria, definition of Section 24(2) penalties, <https://aocsolicitors.com.ng/legal-implications-of-cyber-bullying-and-online-harassment-in-nigeria/> accessed 30 September 2025.

52 *Okedara v. Attorney General of the Federation* (2019) CA/L/174/18 (unreported) decision upholding constitutionality of Section 24(1), <https://globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general/?utm> accessed 30 September 2025.

53 'Punch, report on arrests under cyberstalking Section 24 targeting journalists/critics' <https://punchng.com/how-nigerian-authorities-use-cybercrime-act-to-harass-detain-journalists-activists/> accessed 30 September 2025

The ECOWAS Court ordered Nigeria to amend section 24.[54] That decision influenced the 2024 amendment.

In summary, cyberstalking in Nigeria is now a statutory offence under Section 24 of the Cybercrimes Act (2015) as amended in 2024. Key legal issues include: defining the boundary between legitimate criticism and harassment, ensuring that enforcement of Section 24 respects freedom of speech, aligning Nigeria's law with regional human rights obligations; and building prosecutorial capacity and digital forensics to support convictions.

2.4 CYBERCRIME IN NIGERIA

Cybercrime in Nigeria is one of the most pressing legal and social challenges confronting the nation in the digital age. With the expansion of internet access, smartphones, and e-commerce platforms, Nigeria has witnessed both the benefits of digital transformation and the darker side of cyber-enabled criminality. Ajayi observes that while ICT development has accelerated business and governance, it has equally created a fertile ground for crimes such as phishing, hacking, identity theft, and online scams.[55]

Historically, cybercrime in Nigeria is rooted in the infamous 419 scams, which pre-date widespread internet access but later migrated online with global reach. These scams, criminalized under section 419 of the Criminal Code, involve obtaining property by false pretence. Iorliam notes that this early form of cyber-enabled fraud gave Nigeria an

---

[54] CARJ / ECOWAS Court order 2022: Section 24(1) found arbitrary and violating free speech; Nigeria ordered to amend. Reported by SERAP and Freedom House, e.g. SERAP commentary <https://serap-nigeria.org/2025/01/12/serap-takes-tinubu-govt-governors-to-ecowas-court-over-misuse-of-cybercrimes-act/> accessed 30 September 2025

[55] OA Ajayi, 'Internet Technologies and Cybersecurity Law in Nigeria' (Malthouse Press, Lagos 2024) 45–68 <https://www.africanbookscollective.com/books/internet-technologies-and-cybersecurity-law-in-nigeria> accessed 23 September 2025.

unfortunate reputation as a hub of internet fraudsters, a stigma that continues to influence the country's international image today.[56]

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 remains the cornerstone of Nigeria's legal response. It criminalizes a wide range of offences, including cyberstalking, unlawful access, child pornography, and system interference. Nwafor explains that while the Act is comprehensive, enforcement is hampered by ambiguities, overlapping mandates between agencies, and difficulties with digital evidence preservation.[57] Courts often struggle with admissibility of electronically generated evidence, despite statutory reforms, which weakens prosecutorial outcomes.

Recent studies emphasize the economic dimension of cybercrime. Sibe and Kaunert highlight how Nigerian banks and corporate entities suffer substantial losses through business email compromise, ATM fraud, and digital financial scams.[58] The cost is not only monetary but reputational, as foreign investors and international partners frequently cite cyber insecurity as a factor discouraging engagement with Nigeria. According to Ajayi, these losses exacerbate unemployment and poverty by discouraging investment and increasing transaction costs.[59] Institutionally, agencies such as the Economic and Financial Crimes Commission (EFCC), the Nigerian Police Force, and the National Information Technology Development Agency (NITDA) are central to combating cybercrime. However, Nwafor underscores that weak inter-agency collaboration,

---

56 A Iorliam, 'Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime' (SpringerBriefs in Cybersecurity, Cham 2019) 12–30 <https://link.springer.com/book/10.1007/978-3-030-15210-9> accessed 23 September 2025.

57 IE Nwafor, 'Cybercrime and the Law: Issues and Developments in Nigeria' (Centre for Law and Development Studies, Enugu 2022) 81–105 <https://clds-ng.com/product/cybercrime-and-the-law-issues-and-developments-in-nigeria/> accessed 23 September 2025.

58 RT Sibe and C Kaunert, 'Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria' (Springer, Cham 2024) 95–120 <https://link.springer.com/book/10.1007/978-3-031-54089-9> accessed 23 September 2025.

59 Ibid (n7)

inadequate training of investigators, and corruption remain stumbling blocks.[60] The EFCC has secured high-profile convictions, such as the case of Obinwanne Okeke "Invictus Obi"[61], but such successes are rare compared to the scale of cybercrime.

Scholars stress the need for a holistic approach. Iorliam advocates for improved digital literacy, public awareness campaigns, and international cooperation, especially as most cybercrime activities transcend borders.[62] Sibe and Kaunert further argue for forensic readiness, developing technical and institutional capacity to detect, investigate, and prosecute digital crimes swiftly.[63]

In conclusion, cybercrime in Nigeria reflects a dual reality, the opportunities of digital growth and the vulnerabilities of weak governance structures. While the Cybercrimes Act provides a necessary framework, its success depends on consistent enforcement, judicial capacity, and socio-economic reforms. Without tackling root causes such as unemployment and institutional weakness, cybercrime will remain a persistent challenge to Nigeria's security, economy, and international reputation.

2.5 THEORETICAL FRAMEWORK

2.5.1 Routine Activity Theory

Routine Activity Theory Developed by Lawrence Cohen and Marcus Felson (1979). This is a crime opportunity theory that posits that a crime occurs when three elements converge in time and space: Firstly, a motivated offender, Secondly, a suitable target, and

---

60 Ibid (n9)

61 U.S. Department of Justice, 'Nigerian National Sentenced to Prison for $11 Million Global Fraud Scheme' (2021) <https://www.justice.gov/usao-edva/pr/nigerian-national-sentenced-prison-11-million-global-fraud-scheme.> accessed 23 September 2025

62 Ibid (n8)

63 Ibid (n10)

Lastly is the absence of a capable guardian.[64] In the RAT model, crime does not necessarily depend on long term social or personal dispositions but on everyday routines that bring offenders into contact with targets in contexts where no protective interventions occur. The theory has been widely used to analyze cybercrime, for instance, it suggests that cybercriminals are "motivated offenders" who exploit opportunities like unsecured networks or uninformed users to attack "suitable targets" such as servers, individuals or companies with valuable data when guardians like firewalls, laws or vigilant network monitors are absent or ineffective.

In practice, RAT implies that reducing cybercrime can involve changing any of the three elements. For example, if potential targets like users or systems make themselves less attractive through better security habits, data encryption, or removing unnecessary targets, or if capable guardians such as active cybersecurity monitoring or law enforcement cyber patrols are present, the risk of crime falls even if motivated offenders exist. Nigerian studies have applied RAT by observing how 419 scammers seek out gullible victims online often without robust digital surveillance .[65] The rise of e-commerce and mobile banking in Nigeria has increased the number of high value targets like bank accounts and mobile wallets available, sometimes with limited oversight by financial institutions, thus fitting the RAT framework. On the flip side, initiatives like the Cybercrime Advisory Council and public awareness campaigns can be seen as attempts to introduce guardianship to cyberspace. Empirical research in Nigeria suggests that strengthening guardianship by ways through police hotlines, system monitoring and reducing target

---

64 Ayesh Perera, 'Routine Activities Theory: Definition & Examples' <https://www.simplypsychology.org/routine-activities-theory.html#:~:text=,three factors leads to crime> accessed 24 September 2025

65 M Bello and M Griffiths, 'Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable are Law Enforcement Agencies?' <https://www.researchgate.net/publication/346425621_Routine_Activity_Theory_and_Cybercrime_Investigation_in_Nigeria_How_Capable_Are_Law_Enforcement_Agencies#:~:text=Advisory%20Council%20in%20Nigeria,what%20elements%20make%20a%20target> accessed 23 September 2025.

attractiveness like requiring bank details, NIN verification could disrupt the cybercrime opportunity structure in line with Routine Activity Theory.

2.5.2 Deterrence Theory

Deterrence Theory is a classic principle of criminal law and penology which holds that crime can be prevented by instilling a fear of punishment. In other words, individuals will refrain from offending if they perceive that the costs or penalties outweigh the benefits. This idea goes back to Cesare Beccaria and Jeremy Bentham in the 18th century, who argued that law and punishment should aim to deter future crimes rather than simply to exact retribution. Modern deterrence theory emphasizes two key dimensions. They are; certainty of punishment that is the likelihood of being caught and penalized and severity of punishment, which is how harsh the penalty is. A core insight from empirical research including U.S. studies is that the certainty of punishment tends to have a stronger deterrent effect than the severity of punishment.[66] That is, potential offenders are more dissuaded by a high chance of being caught than by the prospect of a very long sentence.

Applied to cybercrime, deterrence suggests that well publicized investigations and prosecutions can discourage would-be cyber offenders. If cybercriminals believe Nigerian cyber laws are enforced swiftly and that digital forensics will link them to their crimes, they may be deterred from attacking. Nigeria's Cybercrimes Act 2015, for example, imposes significant penalties including multi-year jail terms and large fines for offenses like hacking, fraud and cyberterrorism , embodying the principle of severe punishment. Section 24 of the Act, for instance, makes cyberstalking punishable by up to three years imprisonment. However, actual deterrence also depends on enforcement, if cybercriminals perceive that law enforcement has little capacity to catch them, then even severe legal provisions may have limited effect. In this regard, experts note that

[66] National Institute of Justice, 'Office of Justice Programs (OJP)' <https://nij.ojp.gov> accessed 24 September 2025.

increasing Nigerian police cybercapabilities like improving guardianship and publicizing convictions which includes increasing certainty may do more to deter than simply toughening penalties. As the saying goes: "the certainty of being caught deters a person from committing crime, not the fear of being punished or the severity of the punishment". Thus, Deterrence Theory in the Nigerian context underlines the need for effective policing and robust judicial follow through, not just new laws.

2.5.3 Social Learning Theory

Social Learning Theory often traced to Albert Bandura, 1977, proposes that criminal behavior is learned in much the same way as non-criminal behavior through observing others and modeling their actions. People acquire new behaviors by watching models such as peers, family, media and imitating those behaviors, especially if they see them being rewarded. In a criminal context, this means that individuals may learn how to commit cybercrimes by interacting with others who engage in hacking or fraud, or by absorbing the techniques circulating in online forums. The theory holds that cognitive processes also play a role, for example, a potential offender might pay attention to the outcomes of others' crime and the ease of profits that comes out, remember the steps involved, and then choose to imitate them if it seems advantageous.[67]

In Nigeria, Social Learning Theory helps explain the subculture sometimes called Yahoo Boys, whereby young Nigerians learn online scamming techniques through peer networks and media portrayals. If more experienced fraudsters mentor novices, for example, by showing them phishing tricks or teaching them to clone ATM cards, those novices can internalize and repeat those criminal behaviors. The public response whether society condemns or glamorizes these acts also influences learning. Criminal networks

---

[67] Saul McLeod, 'Albert Bandura's Social Learning Theory' <https://www.simplypsychology.org/bandura.html#:~:text=What%20is%20Social%20Learning%20Theory?> accessed 23 September 2025.

may reinforce each other's skills, creating an environment in which cyber-offenses are normalized. This theory suggests that preventing cybercrime may involve breaking the transmission of criminal knowledge for instance, through education, rehabilitation programs, and changing attitudes so that cyber-offending is no longer seen as a quick path to success. It also implies that individuals under strong positive influences like school, family, work and with role models who emphasize lawfulness are less likely to engage in cybercrime, because they have learned and internalized prosocial behaviors.

2.6 CAUSES OF CYBERCRIME IN NIGERIA

Cybercrime, as stated, is very prevalent in Nigeria, hence there is need to discuss the reasons or causes of cybercrime in Nigeria. In view of the above, the following causes of cybercrime have been identified;

2.6.1 Urbanization

Urbanization has emerged as one of the central socio-economic factors driving cybercrime in Nigeria. The country has experienced rapid demographic shifts, with a rising urban population now estimated at over 50% of the national total. The accelerated growth of cities, without a commensurate expansion in infrastructure, employment opportunities, and law enforcement capacity, has created a fertile environment for crime. In particular, cybercrime has flourished in urban centres, where access to internet facilities is widespread, social anonymity is greater, and competition for limited resources fuels desperation among young people. Scholars have observed that Nigerian cities, while offering access to modern technology, often fail to provide the socio-economic stability that would prevent individuals from resorting to cybercrime as an alternative survival strategy.[68]

---

[68] J Garuba, 'An Approach to Cybercrime Issues Dandume Local Government Area of Kastina State Nigeria' <https://www.ajol.info/index.php/njt/article/download/252681/238749> accessed 30 September 2025.

A major way in which urbanization contributes to cybercrime is through the increased availability of internet access in public spaces such as cyber cafes, shared devices, and informal digital hubs. These access points, often poorly regulated, provide opportunities for cybercriminals to operate with relative ease. Olivia argue that the growing youth population in Nigeria's cities, faced with inadequate jobs and idle time, turn to cyber-enabled fraud because of its low entry requirements and high potential for financial reward.[69] Urban anonymity also weakens traditional social controls, in large cities, individuals can act with a sense of invisibility, making illicit activities like online scams and hacking appear less risky than conventional crime.[70]

Another dimension is the socio-economic disparity that urbanization highlights. The cost of living in Nigeria's major cities is extremely high, while the income levels of a large proportion of urban dwellers remain low. This creates visible inequality, where the conspicuous display of wealth by elites contrasts with widespread poverty and unemployment. Such conditions, according to criminological studies, fuel relative deprivation, which in turn motivates young people to pursue cybercrime as a means of bridging the socio-economic gap.[71] In fact, a 2024 survey on the Nigerian economy and cybercrime revealed that urbanization, when combined with unemployment and weak law enforcement, significantly correlates with the rise of internet-based fraud in urban centres.[72]

---

69 OE Olivia, 'Examining the Effect of the Elevated Rate of Cybercrime on the Growth and Sustainable Development of Nigeria's Economy' <https://journals.unizik.edu.ng/jcpl/article/download/996/832/2557> accessed 30 September 2025.

70 Ibid

71 S Abdul-Rasheed, 'Cybercrime and Nigeria's External Image: A Critical Assessment' <https://www.jpanafrican.org/docs/vol9no6/9.6-9-Abdual-Rasheed.pdf?utm> accessed 30 September 2025.

72 N Udoinyang & A David, 'Relationship Between Cybercrime and the Nigerian Economy: Causes, Implications and the Path Forward' *Journal of Financial and Business Management Studies* (2024) 22, 31 <https://www.rgnpublications.com/journals/index.php/jfbms/article/view/2667> accessed 30 September 2025.

In conclusion, while urbanization in itself is a sign of modernization, the Nigerian context demonstrates how poorly managed urban growth exacerbates crime. The failure to expand infrastructure, employment, and social services alongside urban expansion has left cities vulnerable to cybercrime. Urbanization thus stands as a root cause not only because it creates opportunities for digital connectivity but also because it exposes the inequalities and social pressures that drive young people into cyber-offending.

2.6.2 Unemployment

Unemployment is one of the most critical socio-economic drivers of cybercrime in Nigeria. The country faces a persistent youth unemployment crisis, with official statistics showing large numbers of educated but jobless individuals especially in urban areas. This creates frustration, social discontent, and temptation to turn to alternative income means. Many unemployed youths, having access to the internet and digital tools, resort to cybercrime as a perceived shortcut to financial survival.[73]

The problem is exacerbated by a mismatch between tertiary education output and labour market demand. Nigerian universities graduate thousands each year, but industries capable of absorbing such graduates are weak due to infrastructural deficits, economic instability, and capital flight. This leaves many graduates underemployed or idle, despite possessing ICT relevant skills which they might repurpose for illicit digital activities.[74] Moreover, the social prestige attached to illicit digital gains makes cybercrime alluring. In several urban youth subcultures, the "Yahoo Yahoo" identity is glamorized in music,

---

[73] 'Nigeria Labour Force Survey Q3 2023: youth aged 15-24 had unemployment rate of 8.6 % in Q3 2023' <https://www.nigerianstat.gov.ng/elibrary/read/1241455> accessed 1 October 2025

[74] OE Omoju & EE Ikihde, 'Empirical Review of Youth-Employment Policies in Nigeria' <https://arxiv.org/abs/2310.07789?utm> accessed 1 October 2025.

social media, and peer groups. With legitimate employment scarce, some youths view cyber fraud as not only economically viable but socially rewarding.[75]

On the policy front, the Nigerian government has instituted several youth employment and skills development programmes such as the National Youth Employment Action Plan and Nigeria Youth Service Corp. However, implementation gaps like poor funding, weak coordination, inadequate oversight limit their effectiveness in reducing youth unemployment vulnerability to cybercrime inducements.[76]

2.6.3 Weak Implementation of Cybercrime Laws

Although Nigeria has enacted the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, which remains the primary legislation regulating cyber offences, its implementation has been widely criticized as ineffective. The weakness of enforcement mechanisms stems from poor institutional capacity, insufficient resources, judicial delays, and gaps within the legislation itself.

A critical limitation lies in the lack of technical expertise and forensic capability among law enforcement agencies. Effective cybercrime prosecution requires advanced knowledge in digital forensics, encryption, and cross-border tracking. However, many investigators, prosecutors, and judges in Nigeria lack adequate training to handle such specialized evidence, leading to frequent collapse of cases in court.[77]

Another problem is the resource deficit faced by enforcement agencies. Agencies such as the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force

---

75 NK Aknai, 'Information and Communication Technology: An Evaluation of Cyber Crimes Laws in Nigeria' <https://www.researchgate.net/publication/379606817_INFORMATION_AND_COMMUNICATION_TECHNOLOGY_AN_EVALUATION_OF_CYBER_CRIMES_LAWS_IN_NIGERIA?utm> accessed 1 October 2025.

76 Alfie Kolawole, 'Cybercrime Legislation in Nigeria: Effectiveness and Gaps' <https://www.researchgate.net/publication/388634111_Cybercrime_Legislation_in_Nigeria_Effectiveness_and_Gaps?utm> accessed 1 October 2025

77 Chaman Law Firm, 'Cyber Crime Prosecution: Breakthrough Challenges in Nigeria' <https://chamanlawfirm.com/9-cyber-crime-prosecution-breakthrough-ch/> accessed 1 October 2025.

often lack sufficient funding for forensic laboratories, secure data storage, and surveillance technologies needed to effectively investigate and prosecute cybercrimes.[78] Judicial bottlenecks also weaken enforcement. The Act vests jurisdiction for cybercrime cases exclusively in the Federal High Court, which is already burdened with heavy caseloads. This has created backlogs, with many cases dragging on for years without resolution. The restricted jurisdiction prevents lower courts from sharing the workload, further stifling timely justice delivery.[79]

Legislative shortcomings compound the problem. While the Act addresses offences such as identity theft, cyberstalking, and phishing, it does not fully capture emerging crimes like sophisticated ransomware attacks, advanced cryptocurrency fraud, or certain forms of cyber harassment. This leaves gaps that offenders can exploit. Moreover, the overlap between older laws such as the Advance Fee Fraud and Other Related Offences Act 2006 and the Cybercrimes Act creates jurisdictional confusion.[80]

Finally, low public awareness and under-reporting significantly hinder enforcement. Many victims do not report cybercrimes due to distrust in the system, ignorance of their rights, or the cumbersome reporting process. Without complaints from victims, law enforcement agencies have fewer opportunities to test and enforce the law effectively.[81]

It follows that although Nigeria possesses a strong statutory framework on paper, the weak implementation of the Cybercrimes Act undermines its deterrent effect. For the

---

78 ProfessionsNG, 'Nigerian Police and Cybercrime: Challenges in Tackling Digital Offences' <https://professions.ng/nigerian-police-and-cybercrime/> accessed 1 October 2025.

79 Victor Chijioke and The Cable, 'Federal Courts Can't Handle Cybercrime Cases Alone, Says Lagos Chief Judge' <https://www.thecable.ng/federal-courts-cant-handle-cybercrime-cases-alone-says-lagos-chief-judge/> accessed 1 October 2025.

80 Timothy Ilegbusi, 'Cybercrime Prosecution in Nigeria: Challenges and Prospects' <https://www.researchgate.net/publication/390941849_CYBERCRIME_PROSECUTION_IN_NIGERIA_CHALLENGES_PROSPECTS> accessed 1 October 2025.

81 AA Dawha, 'Nigeria's Cybercrimes Act: A Shield for the Digital Age?' <https://www.linkedin.com/pulse/nigerias-cybercrimes-act-shield-digital-age-abel-ardo-dawha-iaeng--0oizf> accessed 1 October 2025.

legislation to achieve its intended purpose, institutional reforms, capacity building, and enhanced judicial processes are indispensable.

2.7 LITERATURE REVIEW ON CYBERCRIME

Cybercrime has no single universally accepted definition in Nigeria statute. However, Nigerian academics and legal practitioners broadly agree that it refers to offences committed with the aid of computer systems, networks, or digital technologies, whether as the instrument of crime or the direct target.

Muyiwa B. Afolabi and Agbor Julianah Esoso define cybercrime as the use of computers or other Information Communication Technology devices as well as the internet by individuals to commit crimes in cyberspace.[82] They emphasize common forms such as phishing, identity theft, and hacking, and note that young people constitute the majority of offenders.

Similarly, Abubakar, in his socio-legal study of Jigawa State, defines cybercrime as offences enabled by information technologies, committed largely for financial gain by youths engaged in acts such as hacking, phishing and data misuse.[83] His approach highlights the socio-economic dimension, linking high youth involvement to unemployment and opportunity structures.

Egbo offers a broader doctrinal view, describing cybercrime as any criminal activity that involves a computer, networked device or a network.[84] He argues that cybercrimes may either target computer systems directly like hacking, system interference or use them as

---

82 MB Afolabi and AJ Esoso, 'The Role of Youths in Cybercrime in Nigeria' *South Global Journal of Humanities and Development Studies* Vol. 2, No. 1 (2021) <https://sgojahds.com/index.php/SGOJAHDS/article/view/181> accessed 1 October 2025.

83 A Abubakar, 'Cybercrime in Nigeria: A Socio-Legal Analysis with Focus on Jigawa State' *Global Journal of Arts, Humanities and Social Sciences* Vol. 6, No. 10 (2018) 24–33 <https://gojamss.net/journal/index.php/gojamss/article/view/720> accessed 1 October 2025.

84 C. Egbo, 'A Critical Analysis of the Law Regulating Cybercrimes in Nigeria' (2022) <https://www.researchgate.net/publication/388758753_A_CRITICAL_ANALYSIS_OF_THE_LAW_REGULATING_CYBERCRIMES_IN_NIGERIA> accessed 1 October 2025.

tools to commit conventional crimes such as fraud, dissemination of malware. This analytical distinction clarifies the scope of liability under Nigerian law.

From a legal perspective, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 enumerates offences such as unlawful access, cyberstalking, identity theft and electronic fraud, but it does not provide a single definitive meaning of cybercrime. Similarly Onadeko and Afolayan, in their critical appraisal of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, argue that the legislation fails to provide a single comprehensive definition of cybercrime.[85] This legislative silence, they suggest, compels Nigerian scholars to adopt multi-element definitions that combine statutory lists of offences such as unlawful access, cyberstalking, and system interference with broader conceptual frameworks. Their approach therefore situates the definition of cybercrime in the tension between academic clarity and statutory gaps. Scholars such as Adeleke, Akindipe and David have criticized this absence, noting that the lack of a coherent statutory definition undermines enforcement and international cooperation.[86]

2.8 CYBERCRIME AND ITS IMPLICATION ON NIGERIA'S INTERNATIONAL IMAGE

The prevalence of cybercrime in Nigeria has serious ramifications for how the country is perceived internationally. Over time, repeated reports of large-scale fraud, scams, and digital extortion originating or alleged to originate from Nigeria have contributed to a negative reputation in global circles, undermining trust, investor confidence, diplomatic relations, and soft power.

---

85 OA Onadeko and AF Afolayan, 'A Critical Appraisal of the Cybercrimes Act, 2015' *International Society for the Reform of Criminal Law (ISRCL)* (2018) <https://www.isrcl.com> accessed 23 September 2025.

86 A Adeleke and others, 'A Universal Definition of Cybercrime: The Consequences of Incoherence' *Adeleke University Law Journal* Vol. 1 (2020) <https://aulj.adelekeuniversity.edu.ng/index.php/aulj/article/view/17> accessed 23 September 2025.

One of the key consequences is erosion of international trust in digital and financial transactions involving Nigerians or Nigerian institutions. When foreign partners, businesses, or individuals repeatedly encounter fraud originating from Nigeria like the advance-fee scams, business email compromise, romance scams, they may adopt a risk averse posture. This often leads to increased due diligence costs, stricter constraints on digital engagement, or outright refusal to deal with entities based in Nigeria. Such perceptual barriers constrain cross-border trade, fintech collaboration, and global cooperation in ICT. Research shows that cybercrime exerts an inverse influence on Nigeria's national image, that is, higher rates of cybercrime correlate with a worsening reputation abroad.[87]

Secondly, Nigeria's soft power and diplomatic standing suffer when media reports and international studies frequently place Nigeria in the spotlight as a cyber-fraud hub. This narrative skews broader understandings of Nigeria's developmental achievements, overshadowing innovation, cultural exports, and positive narratives. A critical assessment of Nigeria's external image highlights that cybercrime poses a serious threat to the country's external image and contributes to global scepticism about its commitment to rule of law.[88]

Thirdly, foreign direct investment (FDI) and economic cooperation are negatively impacted. Countries and investors consider political risk, regulatory integrity, and the security of transactions. When Nigeria is associated with high cyber risk, foreign investors may demand higher risk premiums or avoid sectors tied to data, ICT, or cross-

---

87 AD Adejumo and KO Oyeniyi, 'Cybercrime and its Effect on Nation Identity Image: Pragmatic Evidence from Nigeria' PJMI <https://www.journals.airsd.org/index.php/pjmi/article/download/419/180/585> accessed 1 October 2025.

88 MA Yinusa and AL Sulaiman, 'Cybercrime and Nigeria's External Image: A Critical Assessment' <https://www.academia.edu/28649731/Cybercrime_and_Nigerias_External_Image_A_Critical_Assessment> accessed 1 October 2025.

border digital business. A study on Nigeria's foreign relations and soft power diplomacy underscores that cybercrime hinders foreign relations and trade ties, ultimately affecting economic partnerships.[89]

Furthermore, diaspora and individual Nigerians abroad may face stigmatization. Because of persistent stereotypes linking Nigeria to fraud, Nigerians residing or working abroad sometimes contend with suspicion or prejudice in professional and social contexts. This social cost compounds reputation risk at the national scale. Studies examining perceptions of Nigerians in the international community note that cybercrime has contributed to a reputational deficit.[90]

Finally, cybercrime scandals involving high-profile actors intensify reputational damage. Notorious cases such as the conviction of Ramon "Hushpuppi" Abbas, a Nigerian known globally for orchestrating multi-million dollar fraud attract wide media coverage and reinforce negative stereotypes linked to Nigeria.[91]

Nigeria's international image is compromised by its association with cybercrime. The long-term effect is twofold: diminished credibility in global digital ecosystems, and increased barriers to international cooperation in trade, finance, and diplomacy. To reverse this, Nigeria must not only tighten cybercrime enforcement internally, but also engage in strategic international communication, transparency, and cybersecurity diplomacy to rehabilitate its reputation.

2.9 CONCLUSION

---

89 Abdulbasit Imam,, 'Nigeria's Foreign Relations and Soft Power Diplomacy' SSRN paper <https://papers.ssrn.com/sol3/Delivery.cfm/4896432.pdf?abstractid=4896432> accessed 1 October 2025.

90 OD Apeloko and CS Chiamaka, 'Impacts of Cyber Crimes on the Image of Nigeria in the International Community: A Case of the Perceptions of Ghanaians' <https://www.researchgate.net/publication/387886171_Impacts_of_Cyber_Crimes_on_the_Image_of_Nigeria_in_the_International_Community_A_Case_of_the_Perceptions_of_Ghanaians?utm> accessed 1 October 2025

91 'Hushpuppi, Wikipedia (recording his fraud convictions and international notoriety)' <https://en.wikipedia.org/wiki/Hushpuppi> accessed 1 October 2025.

This essay has reviewed the works of authors regarding cybercrime in Nigeria. It has been shown from the above review that as the general population becomes more and more refined in their ICT understanding, there is a strong possibility that cybercrime would become more rampant. Nigeria is ranked as having one of the top electronic crime activities in the world.

From the view of other authors, it has been shown that there are different kinds of cybercrime activities such as hacking, malware, cyber stalking, password sniffing etc.

The research also discussed the nature of cybercrime in Nigeria, its types, causes and effects. It can be said that the nature of cybercrime in Nigeria is continually evolving with the emergence of new technologies. Most cybercrimes in Nigeria are tool cybercrimes in nature. This implies that cyber criminals in Nigeria mostly use the computer and internet as a tool to defraud and harm others instead of targeting the computers. The major types of cybercrime include identity theft, malware, cyber stalking, spam, wiretapping, and password sniffing. These forms of cybercrime are caused by the high rate of unemployment, quest for wealth, and a weak implementation of cybercrime laws. The prevalence of cybercrime has also created a bad image for Nigeria amongst the Committee of Nations as one of the most corrupt nations in the world. This tarnished national image affects the way Nigerians are treated abroad with suspicion and extreme caution as Nigerians are stereotyped to be fraudsters and hence not to be trusted. It was also shown that cybercrime also has an implication in the socio-economic advancement of the country as information flowing from the country is been characterized as questionable because of the criminal element that make it unreliable, inaccurate and untrustworthy.

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORK FOR GRAPPLING CYBERCRIME IN NIGERIA.

3.1 INTRODUCTION

In present day Nigeria, the activities of cyber perpetrators have become a menace to the society. With the advent of modern age, legislatures have been struggling to restructure laws that fit crimes perpetrated by cyber culprit. Originally, there were no precise laws in Nigeria for battling computer crimes. This led to the creation of an ideal environment for lawbreakers to freely operate without any law to fight their criminal activities. It is a general norm that an uncodified crime is not punishable, as provided in Section 36 (12) of the 1999 Constitution Which states thus:

"A person shall not be convicted of a criminal offence unless that offence is defined and the penalty thereof prescribed in a written law; and a written law refers to an Act of the National Assembly or a law of a State"

In view of this, the Cybercrime Act has been promulgated for the injunction, prevention. detection, and prosecution of cybercriminal activities and for other associated matters. Aside the Cybercrime Act, there are laws that indirectly relate to the prosecution of cyber culprits. These relevant laws include: Economic and Financial Crimes Commission (Establishment) Act, Advanced Fee Fraud and Other Fraud Related Offences Act, Money Laundering (Prohibition) Act.

3.2 ECONOMIC AND FINANCIAL CRIMES COMMISSION (ESTABLISHMENT) ACT

The Economic and Financial Crimes Commission (Establishment) Act, 2004 (as amended) serves as one of the most significant legal instruments in Nigeria's fight

against economic and financial crimes. It formally establishes the Economic and Financial Crimes Commission (EFCC) as the lead national agency responsible for combating offences such as money laundering, fraud, and other forms of financial misconduct that threaten the integrity of Nigeria's economy.

Under Section 2(1) of the Act, the Commission is constituted with a Chairman who must be a person of high law enforcement rank and representatives drawn from key institutions such as the Ministries of Finance, Justice, and Foreign Affairs, the Central Bank of Nigeria (CBN), and other related bodies.[1] This broad composition ensures inter-agency coordination and fosters an integrated national response to economic and financial crimes.

According to Section 6 of the Act, the EFCC's functions are extensive. It is mandated to enforce all provisions of the Act and to investigate all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer and credit card fraud, and contract scams.[2] The inclusion of computer credit card fraud within its jurisdiction explicitly extends the EFCC's powers to cyber-enabled offences, demonstrating legislative foresight in addressing the modern realities of digital and internet-based financial crimes. The Act also mandates the Commission to coordinate the enforcement of all laws relating to economic and financial crimes in Nigeria. It is empowered to identify, trace, freeze, confiscate, and seize the proceeds of unlawful activities.[3] Furthermore, it may share intelligence and conduct joint operations with other domestic and international law enforcement agencies, including the CBN, Niger Delta Development Commission (NDDC), and National Intelligence Agency (NIA), in order to track offenders and recover illicit assets across borders.

---

1 Economics and Financial Crimes Commission Act, s2(1).

2 Economics and Financial Crimes Commission Act, s6.

3 Ibid.

In Section 7, the EFCC is granted clear investigative and prosecutorial authority. The provision empowers the Commission to initiate investigations where it suspects that a person or organization has committed any offence under the Act or any other law relating to economic and financial crimes. It also allows for lifestyle and asset investigations, enabling the Commission to probe unexplained wealth and detect illicit enrichment.[4]

Section 17 of the Act specifically addresses money laundering offences, defining them as the concealment, conversion, or transfer of property derived from criminal conduct. Convictions under this section may attract prison terms not less than five years, reflecting the seriousness of such offences.[5] Additionally, Section 34 empowers the EFCC Chairman to apply to court, *ex parte*, for orders to freeze bank accounts suspected of containing the proceeds of crime. Once such an order is granted, financial institutions are legally obliged to furnish the Commission with relevant account records.[6] Similarly, Section 32 makes it an offence to tamper with or obstruct the EFCC's seizure or forfeiture operations, or to fail to comply with court orders relating to attached properties.[7]

Through these provisions, the EFCC Act equips the Commission with robust investigative, preventive, and prosecutorial tools, allowing it to dismantle the financial infrastructure of organized and cyber-related crimes. The ability to freeze assets, trace funds, and prosecute offenders has made the EFCC a central institution in Nigeria's anti-corruption and anti-cybercrime framework.

In practical terms, the EFCC has effectively utilized these powers to prosecute numerous cases involving internet fraud and other cyber-enabled offences. A notable example is

---

4 Economics and Financial Crimes Commission Act, s7.

5 Ibid, s17.

6 Ibid, s34.

7 Ibid, s34.

Harrison Odiawa v. Federal Republic of Nigeria[8], where proceeds from an internet-based scam amounting to approximately USD 2 million were confiscated following prosecution under the Advance Fee Fraud and Other Related Offences Act. This case highlights the Commission's role in tackling cross-border and technologically driven financial crimes.

Despite its achievements, the EFCC's operations are not without criticism. Scholars and practitioners have noted persistent challenges, including institutional overlap with other agencies such as the Independent Corrupt Practices and Other Related Offences Commission (ICPC), as well as issues relating to manpower, technical capacity, and political interference.[9] The Economic and Financial Crimes Commission (EFCC), Nigeria's foremost anti-graft agency, has in recent times faced internal controversies that have raised serious concerns about its credibility. In early 2024, the Commission dismissed twenty-seven of its officers for offences ranging from bribery to misconduct, a decision personally approved by the Chairman, Ola Olukoyede.[10] This development came amid growing public criticism that some EFCC officials were compromising investigations in exchange for financial favours. Shortly after, reports emerged that certain officers were being investigated for failing to account for seized exhibits, including large sums of money and gold bars recovered from suspects.[11] These revelations sparked public outrage, as they undermined the EFCC's image as a watchdog

---

8 [2008] 57 WRN 83

9 IA Jamo, 'The Economic and Financial Crimes Commission (EFCC) and Anti-Corruption Crusade in Nigeria: Success and Challenges' *Gusau International Journal of Management and Social Sciences* (2021) 102–120 <https://www.gijmss.com.ng/index.php/gijmss/article/view/61> accessed 29 October 2025.

10 The Guardian Nigeria, 'EFCC dismisses 27 officers for fraud, misconduct' (2025) <https://guardian.ng/news/nigeria/metro/efcc-dismisses-27-officers-for-fraud-misconduct/> accessed 25 October 2025

11 Business Day Nigeria, 'Scandal rocks EFCC as officers disappear with seized gold, $30,000' (2025) <https://businessday.ng/news/article/scandal-rocks-efcc-as-officers-disappear-with-seized-gold-30000/> accessed 25 October 2025.

against corruption. Similarly, in September 2024, the Commission had to open an internal probe after a viral report alleged that some of its personnel had collected a ₦15 million bribe to drop money-laundering charges against social media influencer Idris Okuneye, popularly known as Bobrisky.[12]

While the EFCC has consistently denied claims of institutional corruption, these recurring scandals highlight deep-rooted issues within the agency. They also call for stricter internal monitoring and accountability mechanisms to ensure that those entrusted with fighting corruption do not themselves become part of the problem.

Nonetheless, the EFCC Act remains a cornerstone of Nigeria's legal architecture against economic and cyber-enabled crimes, establishing a framework through which illicit wealth and online fraud can be effectively investigated, prosecuted, and deterred.

3.3 ADVANCE FEE FRAUD AND OTHER FRAUD RELATED OFFENCES ACT

The Advance Fee Fraud and Other Fraud Related Offences Act, commonly referred to as the 419 Act, represents one of Nigeria's most decisive legislative measures against financial deception and fraudulent schemes. Originally enacted in 1995 and later revised in 2006, the Act specifically targets the notorious advance fee fraud, a criminal enterprise where victims are induced to make upfront payments with false promises of future financial returns. The central aim of the Act, as stated in its preamble, is to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences.[13]

Under Section 1(1), it is an offence for any person, by any false pretence and with intent to defraud, to obtain anything capable of being stolen. This section closely mirrors the former Section 419 of Nigeria's Criminal Code Act, from which the Act derived its

---

12 Vanguard News, 'Alleged ₦15m bribe: EFCC probes own officers; invites Bobrisky, VeryDarkMan for questioning' (2024) <https://www.vanguardngr.com/2024/09/bobrisky-adeyanju-commends-efcc-for-opening-investigation-into-n15m-bribe-allegation/> accessed 25 September 2025.

13 Advance Fee Fraud and Other Fraud Related Offences Act, Cap A6, Laws of the Federation of Nigeria 2006.

popular nickname. The provision criminalizes deceitful schemes where an offender obtains property, benefit, or advantage by making false representations. According to Subsection (2), this extends to situations where the offender causes another person to suffer loss through false pretence, even if no physical transfer of property occurs. Conviction under this section attracts imprisonment of seven (7) to twenty (20) years, reflecting the seriousness with which Nigeria's legal system treats such offences.[14]

The 2006 revision of the Act marked a significant modernization, extending its reach into the digital and telecommunications environment. Part II, titled "*Electronic Telecommunication Offences,*" imposes responsibilities on internet and telecom operators to assist in the detection and prevention of cyber-enabled fraud. Section 12 mandates all service providers to verify and record the full names and residential addresses of their subscribers, maintaining this data for a legally prescribed period. Section 13 further requires operators of Internet cafes and network service providers to install real-time monitoring devices and to furnish subscriber information to law enforcement agencies upon request.[15] These provisions reflect an early legislative recognition of the role of telecommunications infrastructure in facilitating and combating online fraud.

Another important feature of the Act is its provision for restitution to victims of fraud. Under Section 11, courts are empowered to order convicted persons to repay victims an amount equivalent to the loss sustained.[16] This section ensures that justice is not only punitive but also compensatory, seeking to restore victims' losses. Nigerian courts have actively applied this section in practice. In *Abdulakdir Ntiem v. Federal Republic of Nigeria,* the Court of Appeal affirmed a restitution order compelling the appellant to forfeit ₦15 million and make monthly repayments to the defrauded party, relying

[14] Section 1(1)–(2), ibid.

[15] Part II, Sections 12–13, ibid.

[16] Section 11, ibid

squarely on Section 11 of the Act.[17] This judicial approach underscores the restorative dimension of Nigeria's anti-fraud regime, combining punishment with victim redress.

Overall, the Advance Fee Fraud and Other Fraud Related Offences Act remains a cornerstone of Nigeria's legal response to internet scams and economic deception. It criminalizes the classic 419 schemes that once earned Nigeria a reputation for cross-border email fraud and enforces stringent penalties on offenders. More importantly, by incorporating telecommunication related obligations, the Act anticipated the evolving nature of digital fraud long before the Cybercrime (Prohibition, Prevention, etc.) Act, 2015 came into force. Nonetheless, legal commentators have pointed out that while the 419 Act effectively targeted false pretence and advance fee schemes, it lacked adequate provisions for newer data-driven offences such as phishing, identity theft, and malware distribution gaps that were later addressed by the Cybercrime Act.[18]

In essence, the Advance Fee Fraud Act bridges the gap between traditional fraud and the modern age of digital deception. It remains a key legal tool for the Economic and Financial Crimes Commission (EFCC) and other enforcement agencies, ensuring that perpetrators of advance fee scams, whether online or offline, face serious legal consequences while victims receive restitution.

3.4 MONEY LAUNDERING (PROHIBITION) ACT

The Money Laundering (Prevention and Prohibition) Act, 2022 is one of Nigeria's most important legal reforms in the fight against financial crime. It was enacted to replace the earlier Money Laundering (Prohibition) Act, 2011 (as amended) and to bring Nigeria's laws in line with global anti-money laundering standards, especially those set by the

---

17 (2015) LPELR-25867 (CA).

18 OA Onadeko and AF Afolayan, 'A CRITICAL APPRAISAL OF THE CYBERCRIMES ACT, 2015 IN NIGERIA' <https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf#:~:text=was%20made,was%20sentenced%20to%20ten%20years> accessed, 25 October 2025.

Financial Action Task Force (FATF) and the United Nations Convention Against Corruption (UNCAC). The Act strengthens the country's legal and institutional framework for preventing, detecting, and punishing money laundering, particularly as criminals increasingly exploit digital technology and cyber platforms to conceal illicit funds.

Section 2 of the Act extends its application to financial institutions, designated non-financial businesses and professions, and any entity that deals with large cash or electronic transactions. This broader coverage shows that Nigeria now recognizes that money laundering is not limited to banks; it can also occur through real estate, casinos, legal practices, and online marketplaces.[19] To curb this, the Act imposes stronger Know-Your-Customer (KYC) and Customer Due Diligence (CDD) obligations. Financial institutions must identify beneficial owners, keep detailed transaction records, and report suspicious transactions to the Central Bank and Nigerian Financial Intelligence Unit (NFIU).[20]

One of the Act's most significant innovations is its recognition of attempted money laundering and failure to disclose the source of funds as separate criminal offences. This means that prosecution can still proceed even when the underlying offence generating the illegal funds cannot be proven. Section 18 prescribes heavy penalties: individuals will face, on conviction to imprisonment for a term of not less than four years but not more than fourteen years or a fine not less than five times the value of the proceeds of the crime or both. A body corporate who contravenes the provisions is liable on conviction to a fine of not less than five times the value of the funds or the properties acquired as a result of the offence committed .Where the body corporate persists in the commission of

---

19 Money Laundering (Prevention and Prohibition) Act 2022, s 2.

20 Ibid, s 3.

the offence for which it was convicted in the first instance, the regulators may withdraw or revoke the certificate or license of the body corporate.[21] These strict sanctions are designed to deter financial crime and disrupt the financial networks that often support cyber-fraud, terrorism financing, and corruption.

The Act also promotes stronger collaboration among key enforcement institutions such as the Economic and Financial Crimes Commission (EFCC), the Central Bank of Nigeria (CBN), and the NFIU. Section 16 authorizes the EFCC to prosecute money laundering offences, while the NFIU collects and analyses financial intelligence reports. This cooperative structure aligns with FATF Recommendation, which encourages coordination between national agencies and international partners in implementing effective anti-money-laundering measures. [22] However, despite these notable improvements, scholars and policy experts have pointed out several challenges that continue to weaken enforcement. These include low prosecution rates, overlapping institutional mandates, inadequate inter-agency coordination, and limited technical capacity for complex financial analysis.[23] In addition, the persistence of manual reporting systems and the lack of a unified, real-time financial database make it difficult to trace cross-border and cryptocurrency based transactions efficiently.

Nevertheless, the Money Laundering (Prevention and Prohibition) Act, 2022 remains a cornerstone of Nigeria's legal response to financial crime. It represents a strong

---

21 Ibid, s 18.

22 Financial Action Task Force (FATF), 'The FATF Recommendations – International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation' (2023) <https://www.fatf-gafi.org/en/publications/fatf-recommendations.html.> accessed 25 october 2025.

23 Maxwell Smith Ogbotor, 'Effectiveness of Anti-Money Laundering Regulations in the Nigerian Banking Sector' *Journal of Business and African Economy* (2025) pp 1-15. <https://iiardjournals.org/get/JBAE/VOL.%2011%20NO.%206%202025/EFFECTIVENESS%20OF%20ANTI-MONEY%201-15.pdf?utm> accessed 25 october 2025.

commitment to transparency, accountability, and global best practices in combating illicit finance.

3.5 CRIMINAL CODE

The Criminal Code Act, codified as Cap C38 Laws of the Federation of Nigeria 2004, remains one of the cornerstones of Nigeria's criminal justice architecture. Originally enacted in 1916 during the colonial administration, the Code was designed to consolidate and systematize criminal law for the Southern Provinces, later extending to the entire Federation. Despite its colonial origin, the Code continues to serve as the principal reference point for defining crimes and prescribing penalties for most conventional offences in Nigeria.[24]

Importantly, Section 3 of the Act embodies the cardinal doctrine of legality, declaring that nothing constitutes an offence unless it is expressly defined and a penalty prescribed by law. This principle, famously captured in the Latin maxim *nullum crimen sine lege*, has been affirmed by the Supreme Court in *Aoko v. Fagbemi*, where the court struck down a conviction for adultery because the act was not criminalized under the Code.[25] Of particular relevance to contemporary Nigerian society is the Code's treatment of fraud, false pretences, and forgery, which historically formed the basis for prosecuting cyber-fraud before the advent of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Section 419, which prohibits obtaining property by false pretences, gained global notoriety as the legal foundation for prosecuting advance fee fraud or 419 scams.[26] Though originally crafted for traditional fraudulent schemes, Nigerian courts have

---

[24] Criminal Code Act, Cap C38 Laws of the Federation of Nigeria 2004.

[25] (1961) 1 All NLR 400.

[26] Section 419, Criminal Code Act (Cap C38 LFN 2004).

extended its application to internet-based crimes. This judicial elasticity demonstrates how even an early 20th-century statute has adapted to 21st-century realities.[27]

In addition, the provisions on forgery (Sections 465–467) and offences against property (Sections 383–420) have been crucial in addressing crimes such as identity theft, falsified documentation, and unauthorized online fund transfers. In *FRN v. Ibori*[28], the Court of Appeal reaffirmed that even within Nigeria's evolving digital environment, the Criminal Code provisions remain valid in prosecuting economic and financial crimes alongside more modern statutes like the EFCC Act and the Money Laundering (Prevention and Prohibition) Act 2022.

However, the Code has not escaped criticism. Legal scholars argue that its language and structure remain archaic, reflecting a society of physical crimes and tangible property, rather than a globalized digital economy where offences are transnational and intangible. As Obasohan and Akpata observe, the Code was not designed for crimes committed through data networks or algorithms, but rather for acts committed with the hand and seen by the eye.[29] This limitation underscores the necessity of supplementary legislation, particularly the Cybercrimes Act 2015, to address emerging threats that transcend the traditional notion of physical criminal conduct.

Despite these limitations, the Criminal Code Act continues to provide the backbone for criminal adjudication in Nigeria. It remains aligned with constitutional safeguards enshrined under Sections 35 and 36 of the 1999 Constitution (as amended), ensuring due process, fair hearing, and the presumption of innocence. Moreover, its fundamental

---

27 Abayomi Ajibade, 'Causes, Consequences and Control of Online Advance Fee Fraud in Ilorin Metropolis, Nigeria' *De-Centre: Journal of Interdisciplinary Studies* (2025) <https://journals.uj.ac.za/index.php/djis/article/view/4096> accessed 20 October 2025

28 (2014) LPELR-22782(CA)

29 JO Obasohan and R Akpata, 'Cyber crime and Ritualism: An Analysis Under the Criminal Code' <https://www.sciencepublishinggroup.com/article/10.11648/j.ijls.20250803.22?Utm> accessed 25 October 2025

doctrines such as mens rea, causation, and the rule of legality continue to inform judicial interpretation and guide the enforcement of newer statutes. As such, the Code endures not merely as a historical relic but as an evolving instrument, harmonizing Nigeria's criminal law tradition with modern realities.[30]

3.6 NIGERIA EVIDENCE ACT

Effective prosecution of cybercrime in Nigeria depends largely on the admissibility of electronic evidence. The Evidence Act 2011, which repealed the outdated 1945 law, introduced modern rules governing computer-generated documents and data. Section 84 of the Act provides that for any electronic record to be admissible, it must be accompanied by a certificate of authenticity confirming the integrity and reliability of the device or process that produced it. In practice, a party seeking to tender such material such as emails, system logs or digital files must attach a sworn statement by a person with relevant technical knowledge affirming that the computer was regularly used, properly maintained and that the document was produced during its normal operation. Without this certificate, electronic evidence is usually rejected or considered unreliable by the courts.[31]

Judicial interpretation has reinforced the strict application of this rule. In *Kubor v. Dickson*, the Supreme Court held that computer-generated evidence is inadmissible unless the party tendering it satisfies all the requirements of Section 84(2) of the Evidence Act.[32] The Court emphasized that proof of authenticity either through the statutory certificate or credible oral evidence is indispensable. Consequently, compliance with Section 84 has become a trite principle in Nigerian evidence law.

---

30 Ibid.

31 Evidence Act, 2011 (Cap. E14 LFN 2011) s. 84(1)–(4).

32 (2013) 4 NWLR (Pt. 1345) 534 (SC).

Despite this legal advancement, commentators have identified persistent challenges. While Section 84 provides a legal framework for authenticating digital records, Nigeria still lacks adequate digital forensic infrastructure to verify the origin and integrity of electronic evidence.[33] In many cases, parties rely on printed screenshots or basic witness testimony rather than certified digital reports, which falls short of international best practice. Similarly, legal practitioners have warned that the courts remain ill-equipped to assess the authenticity of complex data such as deepfakes, encrypted communications, or tampered metadata.[34]

Thus, while the Evidence Act 2011 represents a major step toward integrating technology into Nigeria's evidentiary system, its practical implementation remains imperfect. The certificate requirement has brought a measure of credibility to digital evidence, yet outdated procedures and limited technical expertise continue to hinder effective prosecution of cybercrime. As one corporate lawyer aptly noted, Nigeria's evidentiary rules are still archaic in technological terms and must evolve to keep pace with modern realities.[35]

3.7 THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT, 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 remains Nigeria's most comprehensive legislative response to the evolving threat of cybercrime. Enacted on 5 May 2015, the statute represents the country's first omnibus law dedicated exclusively to cyber offences. The *Explanatory Memorandum* to the Act sets out its overarching objectives: to provide "an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and

---

33 Fancy Goodman, 'Can Nigerian courts handle AI-generated evidence? Lawyers say it's inevitable' <https://techcabal.com/2025/05/19/can-nigerian-courts-handle-ai-generated-evidence-lawyers-say-its-inevitable/#:~:text=While%20Section%2084%20of%20Nigeria%E2%80%99s,%E2%80%9D> accessed 25 October 2025.

34 Ibid.

35 Ibid.

punishment of cybercrimes in Nigeria."[36] It also aims to protect what it describes as Critical National Information Infrastructure and to ensure the security of computer systems, electronic communications, data, intellectual property and the privacy of users.[37] Before 2015, Nigeria had no single, coherent legal framework addressing cyber offences. Existing statutes, such as the Economic and Financial Crimes Commission (Establishment) Act, the Advance Fee Fraud and Other Related Offences Act, and the Money Laundering (Prohibition) Act, were insufficient to address the emerging dimensions of online crime.[38] As a result, offenders exploited gaps in enforcement, while prosecutors struggled to fit technologically advanced crimes into the confines of outdated statutes. The Cybercrimes Act was therefore conceived to harmonize the nation's legal approach and bring it in line with international best practices.[39]

One of the distinctive features of the 2015 Act is that it does not attempt to define cybercrime in abstract terms. Instead, it enumerates a series of specific offences that collectively capture the range of harmful activities perpetrated through computers and electronic communication networks. The Act contains fifty-nine sections divided into eight parts, dealing respectively with its objects and application, protection of critical infrastructure, offences and penalties, obligations of service providers, enforcement mechanisms, jurisdictional issues, and international cooperation.[40]

---

36 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, Explanatory Memorandum;

37 Ibid.

38 OA Onadeko and AF Afolayan, 'A CRITICAL APPRAISAL OF THE CYBERCRIMES ACT, 2015 IN NIGERIA' <https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf#:~:text=was%20made,was%20sentenced%20to%20ten%20years> accessed, 25 October 2025.

39 E Eboibi, 'A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015' *Delta State University Law Review* (2023) <https://delsulawreview.com/wp-content/uploads/2023/07/3.-A-Critical-Exposition-Of-The-Nigerian-Cybercrimes-Prohibition-Prevention-Etc-Act-2015.pdf?Utm> accessed 25 october 2025

40 Cybercrimes Act 2015, Part I-VIII

Among the notable offences criminalized by the Act are;

a) Illegal system access or hacking (section 6)

b) System interference (section 8)

c) Identity theft (section 22)

d) Cyberstalking (section 24)

e) Cybersquatting (section 25)

f) Cyber-related pornography and child pornography (section 23)

g) Phishing and malware dissemination (section 32) and

h) Forgery (section 13).[41]

The Act also prohibits the possession or distribution of hacking tools or passwords as provided in section 33 of the Act.

Part V and Part VI of the Act strengthen enforcement by conferring extensive investigative powers on law enforcement agencies. For instance, the Act empowers police officers to compel the disclosure of computer access information or to conduct search and seizure of electronic data with judicial authorization. The Act further mandates financial institutions and Internet service providers to report suspicious electronic transactions to relevant authorities an obligation modelled on the compliance framework of the Money Laundering (Prohibition) Act.[42]

Perhaps the most controversial provision of the Act is section 24, which makes it an offence to send any message or content that is grossly offensive, indecent, obscene or menacing in character, or false information sent with the intent to cause annoyance, inconvenience or danger.[43] The penalty for this offence is a fine of up to ₦7 million,

[41] Cybercrimes Act 2015..

[42] Ibid., Part V.

[43] Ibid., s. 24(1)

imprisonment for up to three years, or both.[44] While intended to address cyberstalking and online harassment, this provision has sparked intense constitutional debates about its compatibility with the freedom of expression guaranteed under section 39 of the 1999 Constitution (as amended).

The controversy reached the courts in *Okedara v. Attorney-General of the Federation,* where the appellant challenged the constitutionality of section 24(1) on grounds of vagueness.[45] The Court of Appeal upheld the provision, ruling that the section was clear, precise and not in violation of the constitutional right to freedom of expression. The court reasoned that section 24 imposed a permissible limitation under section 45(1) of the Constitution, which allows restrictions in the interest of public order and morality.[46] Consequently, the Court dismissed the appeal and affirmed the trial court's decision, thereby validating the section's continued enforcement.

In practical terms, the Cybercrimes Act has substantially improved Nigeria's capacity to investigate and prosecute computer-related offences. Its framework aligns with international standards, including the Budapest Convention on Cybercrime, to which Nigeria has expressed adherence through domestic adaptation.[47] However, implementation challenges persist. Law enforcement agencies often lack adequate technical capacity and forensic tools to preserve and analyse digital evidence.[48] In addition, bureaucratic hurdles, limited funding, and the slow pace of judicial processes have all impeded effective prosecution.[49] The Cybercrime Advisory Council, established

---

[44] Ibid., s. 24(2).
[45] *Okedara v. Attorney-General of the Federation* (2019) CA/L/174/18 (Court of Appeal, Lagos Division).
[46] Constitution of the Federal Republic of Nigeria (1999, as amended), s. 45(1).
[47] Council of Europe, "Nigeria and the Budapest Convention on Cybercrime," accessed 25 October 2025
[48] Ngozi Nzoka and Nneka Umejiaku, 'Cybercrime and Digital Transaction Laws in Nigeria: A Review' <file:///C:/Users/eliteclassuser/Downloads/EWS-Uzoka-080-5.pdf> accessed 25 October 2025
[49] OA Onadeko and AF Afolayan, 'A CRITICAL APPRAISAL OF THE CYBERCRIMES ACT, 2015 IN NIGERIA' <https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf#:~:text=was%20made,was%20sentenced%20to%20ten%20years> accessed, 25 October 2025.

under the First Schedule to the Act, has also been criticized for ineffectiveness due to poor coordination and limited institutional authority.[50]

In response to persistent criticisms, the Cybercrimes (Amendment) Act, 2024 was introduced to refine certain provisions of the principal Act. The amendment sought to clarify offences related to cyberterrorism, expand coverage for financial technology crimes, and strengthen data-protection mechanisms.[51] Nonetheless, observers note that while these reforms represent progress, they have not adequately resolved the underlying concerns about definitional vagueness and potential infringement of digital rights.

In conclusion, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 represents a landmark in Nigeria's legal architecture against cyber offences. It consolidates previously fragmented laws, introduces modern enforcement tools, and aligns national policy with global cybersecurity standards. However, for the Act to achieve its full purpose, greater attention must be given to institutional capacity building, procedural safeguards, and rights sensitive interpretation by the courts. The ongoing balance between cybersecurity and civil liberties remains one of the most pressing questions in Nigeria's digital legal evolution.

3.8 THE NIGERIA POLICE ACT, 2020

The Nigeria Police Act, 2020 represents a landmark reform in the country's security and law enforcement architecture. Enacted to repeal the outdated Police Act of 1943, the new legislation aims to modernize police operations, enhance professionalism, and align Nigeria's policing framework with global human rights and democratic standards.[52] The Act serves as a pivotal component of Nigeria's institutional response to emerging crimes,

---

50 Ibid.

51 Templars Law Firm, 'Overview of the Cybercrimes (Amendment) Act 2024' <https://www.templarslaw.com/app/uploads/2024/08/Cybercrimes.pdf?> accessed 25 October 2025.

52 Federal Republic of Nigeria, Police Act, 2020

including cybercrime, terrorism, and organized criminal networks, by strengthening investigative capacity and promoting accountability within the Nigeria Police Force .

Section 4 of the Act outlines the core responsibilities of the police: the prevention and detection of crime, the preservation of law and order, and the protection of life and property. Importantly, the 2020 Act redefines policing in Nigeria by embedding the principle of intelligence-led and technology driven policing, enabling officers to adopt data based and digital tools to respond to modern threats.[53] This reform reflects the shift from reactive enforcement to proactive security management, especially relevant in combating cyber-enabled offences that often transcend geographical and jurisdictional boundaries.

One of the most progressive features of the Police Act, 2020 is the institutionalization of community policing under Part XIV (Sections 113–119). Section 116 expressly provides that the objectives of the Community Policing Committees include maintaining a partnership between the community and the Nigeria Police Force, promoting communication and co-operation, improving police services to communities,and enhancing transparency and accountability in policing.[54] It also facilitates better intelligence gathering and responsiveness to local security challenges, marking a departure from the traditional centralized policing system that had long been criticized for alienating the citizenry.

The Act also strengthens accountability and oversight mechanisms by reinforcing the supervisory role of the Police Service Commission ,mandating fair recruitment, promotion, and discipline procedures to curb corruption and abuse of office. Additionally, Section 1 of the Act expressly obliges the police to respect and protect citizens'

---

53 Section 4, Police Act, 2020.

54 Nigeria, Police Act, 2020, ss 113–119 (Part XIV)

fundamental rights as enshrined in the Constitution of the Federal Republic of Nigeria 1999 (as amended) and relevant international instruments, including the United Nations Code of Conduct for Law Enforcement Officials and the African Charter on Human and Peoples' Rights.[55]

Furthermore, the Act promotes inter-agency cooperation in the fight against complex crimes, particularly cybercrime, money laundering, and terrorism financing. It encourages collaboration between the Nigeria Police Force and agencies such as the Economic and Financial Crimes Commission (EFCC), the National Information Technology Development Agency (NITDA), and the National Cybercrime Centre, facilitating joint intelligence operations and data sharing.[56] This integrated approach enhances Nigeria's overall security governance and its alignment with the global fight against transnational crime.

However, despite these reforms, the Nigeria Police Force continues to face deep-rooted challenges such as inadequate manpower, poor funding, lack of forensic infrastructure, and persistent political interference.[57] These constraints often undermine the operational independence of the police and erode public confidence in law enforcement institutions. Nonetheless, the Police Act, 2020 remains a crucial legal framework for achieving a more professional, transparent, and technologically adaptive police service capable of responding to Nigeria's evolving security landscape.

3.9 THE NIGERIAN FINANCIAL INTELLIGENCE UNIT (NFIU)

The Nigerian Financial Intelligence Unit (NFIU) is Nigeria's central agency responsible for receiving, analysing, and sharing financial intelligence to combat money laundering,

---

55 Section 1, Police Act, 2020.

56 1st Attorneys Legal Insights, 'The Nigerian Police Act 2020: A Framework for Rights, Accountability and Modern Policing' <https://1stattorneys.com/articles/2025/10/23/the-nigerian-police-act-2020-a-framework-for-rights-accountability-and-modern-policing/> accessed 29 October 2025.

57 Ibid.

terrorism financing, and other financial crimes. Originally established in 2004 as a department within the Economic and Financial Crimes Commission (EFCC), the NFIU was made fully independent through the Nigerian Financial Intelligence Unit (Establishment) Act, 2018 after Nigeria's suspension from the Egmont Group in 2017 due to concerns about its lack of autonomy.[58]

The Act vests the NFIU with authority to collect, analyse, and disseminate intelligence reports to competent authorities such as the EFCC, ICPC, DSS, and the Nigeria Police Force.[59] It also mandates financial institutions and designated non-financial businesses to submit suspicious transaction reports and comply with anti-money laundering and counter-terrorism financing regulations.[60] By aligning with Financial Action Task Force (FATF) standards, Nigeria strengthened its global credibility in the fight against illicit financial flows. Despite notable progress, the NFIU faces challenges including manpower shortages, weak technical capacity, and resistance from some public institutions.[61] Furthermore, its lack of prosecutorial powers limits enforcement, as it must rely on other agencies to act on its intelligence reports. Nonetheless, the NFIU remains a vital component of Nigeria's anti-financial crime framework, fostering both domestic coordination and international cooperation in tackling illicit financial activities.

3.10 NIGERIAN CYBERCRIME WORKING GROUP

The Nigerian Federal government in 2004 set up the Nigeria Cybercrime Working (NCWG) to realize the objectives of National Cybersecurity Initiative (NCI).[62] The

---

58 Nigerian Financial Intelligence Unit (Establishment) Act 2018

59 Ibid., ss. 4–6.

60 Money Laundering (Prevention and Prohibition) Act 2022, s. 7.

61 HP Faga, 'An Examination of the Nigerian Financial Intelligence Unit' *African Journal of Criminal Law and Jurisprudence* (2024) <file:///C:/Users/eliteclassuser/Downloads/2952-3777-1-PB.pdf> accessed 26 October 2025.

62 MU Maska, 'Building National Cybersecurity Capacity in Nigeria: The Journey So Far (presentation, ITU-D Tunis, June 2009) <https://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf> accessed 26 october 2025

objectives of the NCI comprised of public education of the Nigerian masses on the nature and risk/endangerment of cybercrime, criminalization through new legislation of all online vices, formation of legal and technical framework to protect computer systems and Networks, and security of critical information infrastructure for the country. The group was established to deliberate on and suggest ways of confronting the condition of internet fraud in Nigeria.

3.11 CONCLUSION

This essay has deliberated on the various Acts and institutions regulating cybercrime in Nigeria, aside the Cybercrime Act, though these various laws and institutions are not perfectly operative, they would go a long way in battling mainly internet-related fraud. In particular, as a result of the enacted Cybercrime Act 2015, Nigeria can now affirm that a legislation is in place for the purpose of tackling cybercrimes.

CHAPTER FOUR

POTENCY OF THE LEGAL FRAMEWORK FOR GRAPPLING CYBERCRIME IN NIGERIA.

4.1 INTRODUCTION

In today's digital world, the link between technology and crime has become increasingly strong. Cybercrime broadly defined as the use of computers, networks, or other information and communication technologies (ICT) to commit or facilitate offences poses serious threats to national security, economic stability, and individual rights. For developing countries like Nigeria, these challenges are particularly severe. While rapid technological growth has brought new opportunities, it has also exposed gaps in infrastructure, legislation, and enforcement. Limited technical capacity and institutional weaknesses continue to make it difficult for Nigeria to keep pace with the constantly evolving nature of cyber threats.

This chapter examines how effective Nigeria's legal framework is in addressing these challenges. It focuses on the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 the nation's principal law on cyber offences and evaluates its strengths, shortcomings, and implementation gaps. It also compares Nigeria's framework with international standards and highlights the operational and technical difficulties that hinder enforcement.

The goal is to assess not just the adequacy of the law, but how well it works in practice. Key questions guide the discussion: How does Nigeria's framework compare with those of leading jurisdictions? What gaps remain in the Cybercrime Act and related regulations? What enforcement challenges persist? And ultimately, what reforms are needed to build a stronger and more responsive legal system against cybercrime in Nigeria?

4.2 LEGAL FRAMEWORK ON CYBERCRIME IN OTHER JURISDICTIONS

4.2.1 The United States

The United States presents one of the most extensive and sophisticated legal frameworks for addressing cybercrime in the world. Its system, developed over decades of legislative refinement, enforcement experience, and public–private collaboration, has positioned the country as a global benchmark in combating cyber threats. The foundation of this framework lies primarily in the Computer Fraud and Abuse Act (CFAA) of 1986, codified under 18 U.S.C. §1030, which remains the cornerstone of federal cybercrime law. The Act criminalizes a broad spectrum of conduct, including unauthorized access to computer systems, the transmission of malicious software, data theft, and various forms of computer-related fraud.[1] It also extends to the trafficking of passwords and threats involving computer systems, thereby providing a comprehensive coverage of offences that arise within the digital ecosystem. Over time, the CFAA has undergone numerous amendments to accommodate evolving technological realities and emerging forms of cyber misconduct. Its strength lies in its wide jurisdictional reach, which extends to any protected computer used in interstate or foreign commerce, allowing U.S. authorities to prosecute offences that have transnational elements.[2] In addition to the CFAA, the United States has developed a network of complementary federal statutes that address specific dimensions of cybercrime. These include laws on identity theft, electronic espionage, data protection, and the Cybersecurity Information Sharing Act (CISA) of 2015, which facilitates the sharing of cyber threat intelligence between government and private

---

1 18 U.S.C. § 1030 — Fraud and related activity in connection with computers. <https://www.law.cornell.edu/uscode/text/18/1030> Accessed 2 November 2025.

2 Every CRS Report for Congress, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Act (CFAA) (2023). <https://www.everycrsreport.com/reports/97-1025.html> Accessed 2 November 2025.

entities.[3] The rationale behind this collaboration is simple yet critical, most digital infrastructure in the U.S. is privately owned, making cooperative engagement indispensable for a resilient cybersecurity ecosystem.

Institutionally, enforcement in the United States involves several specialized agencies, the most notable being the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ). Each agency maintains dedicated cyber divisions that investigate offences, prosecute offenders, and coordinate with international partners such as INTERPOL and the Council of Europe. The Internet Crime Complaint Center (IC3), operated by the FBI, received 859,532 cybercrime complaints in its 2024 report, with total reported losses exceeding 16 billion U.S. dollars, marking a 33 percent increase from the previous year.[4]These statistics reveal not only the increasing economic cost of cybercrime but also the growing efficiency of detection and reporting systems in the United States.

Several distinct features make the American framework an invaluable point of comparison for Nigeria. Firstly, the clarity of offence definition under statutes such as the CFAA ensures that both law enforcement and the judiciary can apply the law consistently. Secondly, the extraterritorial jurisdiction of U.S. cyber laws demonstrates the importance of protecting citizens and national networks from foreign based attacks, an element particularly relevant to Nigeria given the transnational nature of cyber threats. Thirdly, the obligations placed on private sector entities, such as mandatory breach notifications and data protection duties, underline the shared responsibility in cybersecurity management. Lastly, the rigorous enforcement regime, characterized by high-profile prosecutions and substantial penalties, serves as a deterrent and reinforces institutional credibility.

---

3 Cybersecurity Information Sharing Act of 2015,

4 Federal Bureau of Investigation, Internet Crime Report 2024.<https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>Accessed 2 November 2025.

Nonetheless, the American system is not without criticism. Scholars and civil liberties advocates have long contended that the CFAA is overly broad and risks criminalizing non-malicious or exploratory digital behavior.[5] The law's phrase exceeding authorized access has, in some cases, been interpreted too expansively, prompting the U.S. Supreme Court to narrow its meaning in *Van Buren v. United States*[6], holding that mere misuse of authorized access does not necessarily constitute a federal crime.[7] Furthermore, the United States continues to grapple with the challenge of cross-border evidence collection, balancing privacy rights with national security, and keeping pace with emerging threats such as artificial intelligence, deepfakes, and cryptocurrency-based crimes. These experiences underscore an important lesson for Nigeria: effective legal response to cybercrime must extend beyond statutory enactments to include adaptive governance, institutional capacity, and continuous technological learning.

4.2.2 England

The English legal system provides another significant model for understanding cybercrime regulation, with an emphasis on legislative clarity, institutional coordination, and regular statutory review. The central statute in this regard is the Computer Misuse Act (CMA) of 1990, which remains the foundation of the United Kingdom's cybercrime framework.[8] The Act criminalizes unauthorized access to computer systems under Section 1, access with intent to commit further offences under Section 2, and acts intended to impair or hinder the operation of computers under Section 3. This tripartite structure provides a layered understanding of cyber offences, differentiating between

---

5 John Villasenor, 'Reining in overly broad interpretations of the Computer Fraud and Abuse Act' <https://www.brookings.edu/articles/reining-in-overly-broad-interpretations-of-the-computer-fraud-and-abuse-act> Accessed 2 November 2025.

6 (2021) 141 S Ct 1648

7 Ibid.

8 Computer Misuse Act 1990 (UK), < https://www.legislation.gov.uk/ukpga/1990/18/contents> Accessed 2 November 2025.

minor intrusions and acts of serious harm such as denial-of-service attacks or system sabotage. The CMA has since been supplemented by newer legislation and regulatory guidance to keep pace with evolving threats. Most notably, the Online Safety Act 2023 addresses harmful online behavior, while the Crown Prosecution Service (CPS) has issued updated prosecutorial guidelines distinguishing between cyber-dependent and cyber-enabled crimes.[9] Cyber-dependent crimes refer to those that can only be committed using computers or networks, such as hacking and malware distribution, while cyber-enabled crimes are traditional offences like fraud and harassment that have been amplified through digital technologies.[10] This conceptual distinction provides clarity for prosecutors, enhances law enforcement focus, and allows for a more effective allocation of resources in combating different types of cybercrime.

From a policy perspective, the United Kingdom places significant emphasis on public-private cooperation and the protection of Critical National Infrastructure (CNI). Given that cyber threats often target essential services such as energy, transport, and communication systems, the government has adopted a holistic security strategy that integrates private stakeholders into the national cybersecurity framework. The UK's participation in the Budapest Convention on Cybercrime further reflects its commitment to international collaboration, particularly in the areas of evidence sharing, cross-border investigation, and extradition. The ongoing Review of the Computer Misuse Act, alongside proposals for tougher penalties including life imprisonment for cyber attacks causing catastrophic damage demonstrates the UK's proactive and dynamic approach to law reform.[11]

---

9 Crown Prosecution Service, Guidance on Computer Misuse Act 1990. <https://www.cps.gov.uk/legal-guidance/computer-misuse-act> Accessed 2 November 2025.

10 Ibid.

11 Ibid.

Empirical data from the Cyber Security Breaches Survey 2024 indicated that approximately 22 percent of UK businesses and 14 percent of charities experienced a cyber incident within a twelve-month period, with figures rising sharply among medium and large enterprises.[12] Yet despite these alarming statistics, referrals for prosecution under the CMA have declined, underscoring a persistent enforcement gap.[13] This gap reflects institutional limitations, resource constraints, and procedural bottlenecks, a reminder that strong laws alone are insufficient without robust implementation capacity.

The English framework provides several valuable lessons for Nigeria. Firstly, it highlights the importance of differentiating between various categories of cyber offences, ensuring that enforcement remains proportional and context sensitive. Secondly, it shows that clear prosecutorial guidance can promote consistency and reduce arbitrary enforcement. Thirdly, the UK's commitment to periodic legislative review is a model for how Nigeria can ensure that its cybercrime laws remain technologically relevant. Finally, the English experience demonstrates the necessity of international collaboration, since cybercrime is inherently transnational.

However, like the United States, the United Kingdom also faces challenges. The rapid evolution of technology especially in the areas of encryption, artificial intelligence, and cryptocurrencies poses significant hurdles to investigation and lawmaking. Furthermore, while data collection on cyber incidents has improved, the categorization and reporting of cybercrime statistics remain inconsistent.[14] These limitations reveal the underlying truth that the effectiveness of any cybercrime regime rests not merely on statutory text but on institutional adaptability, technological competence, and sustained inter-agency cooperation.

---

[12] UK Department for Science, Innovation and Technology, Cyber Security Breaches Survey 2024.<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024> Accessed 2 November 2025.

4.3 LOOPHOLES OF THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT 2015

Despite being celebrated as Nigeria's flagship law for combating digital offences, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 has continued to attract criticism from scholars, legal practitioners, and human rights advocates. Although the Act represented a major legislative step forward when it was enacted, it has not fully lived up to expectations. Its shortcomings ranging from vague definitions to weak enforcement structures have weakened its potency and created room for abuse, poor coordination, and ineffective prosecution. To understand these gaps more clearly, this section highlights the major areas where the Act falls short and explains how those weaknesses have shaped Nigeria's struggle against cybercrime.

4.3.1 Lack of Clear Definition and Scope of Offences

A key challenge in the Act lies in its lack of clarity and comprehensiveness in defining core cybercrime concepts. While the Act criminalizes a number of offences such as hacking, identity theft, and cyberstalking, its language remains imprecise and sometimes outdated. As John Odey observes,"the Act is not elaborate in enumerating acts and activities that constitute cybercrimes."[13] For instance, Section 6(1) of the Act links unauthorized access to data that are vital to national security. This narrow framing implies that unauthorized access to systems not tied to national security may escape criminalization, even though such access could still result in severe economic or personal

[13] John Odey, 'Issues Confronting the Effective Administration of Cybercrime Law in Nigeria :Legal Loopholes, Law Axis 360', <https://mylawaxis360.wordpress.com/2021/06/24/issues-confronting-the-effective-administration-of-cybercrime-law-in-nigeria/> Accessed 2 November 2025.

harm.[14] Similarly, Section 10 limits the offence of tampering with critical infrastructure to persons employed by or working under a local government, private organization, or financial institution leaving a loophole for external actors or independent contractors who engage in similar misconduct.[15]

Beyond these drafting issues, the Act fails to capture emerging forms of cyber threats that have evolved rapidly since 2015. Crimes involving deepfakes, cryptocurrency-based fraud, artificial intelligence manipulation, botnets, and cloud-related breaches are not expressly mentioned in the statute.[16] As a result, law enforcement agencies often struggle to interpret or prosecute such offences, since the provisions were written for a much earlier digital context. This lack of technical depth in the law shows how static legislation can become outdated in a dynamic cyber ecosystem. Without constant legislative review and modernization, new categories of cybercriminal activity such as crypto-based Ponzi schemes or AI-generated disinformation may continue to flourish unchecked.

4.3.2 Institutional and Enforcement Ambiguities

Another major weakness of the Cybercrime Act is its institutional vagueness. The Act does not clearly assign responsibility for enforcement to a specific agency. Instead, it vaguely refers to relevant law enforcement agencies without explicitly identifying which institutions should lead or coordinate cybercrime investigations.[17] This ambiguity has produced overlaps, rivalry, and confusion among Nigeria's security and regulatory bodies.

---

14 Ibid.

15 Ibid.

16 O A Onadeko & A F Afolayan, 'A Critical Appraisal of the Cybercrimes Act, 2015' (2018) International Society for the Reform of Criminal Law (ISRCL)< https://www.isrcl.com> Accessed 2 November 2025.

17 Charity Chinedu-Uhuo & Paschal Oguguo Olebara, 'A Comparative Analysis of the Legal Framework on Cybercrime in Nigeria With United State of America, Canada and Egypt' <https://www.nigerianjournalsonline.com/index.php/AEFULJ/article/download/5397/6531> Accessed 2 November 2025.

Agencies such as the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), and the Nigerian Communications Commission (NCC) all claim jurisdiction in cybercrime matters. In practice, this has resulted in duplication of duties, turf battles, and inconsistent investigative outcomes. Furthermore, the administration of the National Cybersecurity Fund under Section 44 of the Act is riddled with administrative opacity. The Act imposes levies on financial institutions to fund cybersecurity efforts, but it offers no clear mechanism for collection, oversight, or accountability.[18] There is ambiguity in levy collection, oversight, and use of funds regarding constitutional consistency, some sections are outdated and do not reflect current Internet access methods.[19]

This institutional confusion undermines the operational side of cybercrime control, as funds meant for technological upgrades, capacity building, and awareness programmes often remain mismanaged or unutilized. Without a clear structure and accountability mechanism, even a well written law will struggle to achieve its intended impact.

4.3.3 Rights, Freedom of Expression, and Over-Broad Offences

Perhaps the most controversial part of the Cybercrime Act is Section 24, which deals with cyberstalking and the sending of offensive or false messages. The provision has long been criticized for being vaguely worded and for its potential to infringe on constitutional freedoms. It criminalizes any message that is grossly offensive or false and sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury,

[18] Ngozi Egenuka 'Cybercrimes Act: Still a long way to curbing cyberspace-related crimes' <https://guardian.ng/technology/cybercrime-act-still-a-long-way-to-curbing-cyberspace-related-crimes/>Accessed 2 Novemebr 2025.

[19] Ibid.

criminal intimidation, enmity, hatred, ill-will or needless anxiety.[20] Such subjective language opens the door for arbitrary interpretation and misuse against journalists, bloggers, political critics, or private citizens expressing dissenting views online. Indeed, several Nigerian courts have heard cases where this section was used to target citizens for allegedly offensive social media posts. Although the 2024 amendments attempted to refine this section by narrowing it to cases that may cause a breakdown of law and order or pose a threat to life, human rights advocates maintain that the provision still grants excessive discretion to law enforcement agencies.[21] It continues to raise constitutional questions about the balance between cybersecurity regulation and freedom of expression under Section 39 of the 1999 Constitution.

This tension illustrates the broader challenge of digital regulation protecting citizens from online harm while safeguarding fundamental rights in cyberspace. A democratic digital regime must ensure that laws against cyber abuse do not become tools of suppression.

4.3.4 Technological, Evidential, and Procedural Limitations

Even in situations where cyber-offences are clearly defined on paper, the reality on the ground in Nigeria is far more troubled. Cybercrime prosecutions depend heavily on digital evidence data that is by its nature fragile, ephemeral and easily manipulated, encrypted or erased long before the courtroom sees it. Yet Nigeria continues to struggle with significant institutional deficits, the number of fully equipped forensic laboratories remains low, law enforcement and prosecuting agencies lack sufficient numbers of trained personnel in computer forensics, and there is no dedicated cybercrime court

---

[20] Oyetibo Tayo (SAN), 'The Constitutionality and Legality of the Cybercrimes Act in Nigeria'<https://www.vanguardngr.com/2024/05/controversial-cybercrime-law-the-way-out-by-lawyers/ >Accessed 2 November 2025.

[21] Ibid.

infrastructure widely established.[22] These weaknesses mean that many cybercrime investigations, no matter how promising initially, fall apart in court because of broken chains of custody, inadequate forensic analysis, or misinterpretation of technical data. This was illustrated in the Nigerian case of *Julius v. FRN*. In that matter, the appellant, Mr Raymond Akolo Julius, was prosecuted under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 for publishing a message on his Facebook platform. While the Court of Appeal upheld his conviction for one count of computer-related forgery under section 13 of the Act, it overturned several other counts because the prosecution failed to establish key technical and evidential elements.[23] For example, the court found that the prosecution had not shown the computer system or network in question was a designated computer system or a piece of Critical National Information Infrastructure (CNII) as required under the Act. That gap alone collapsed significant parts of the case. The decision powerfully underscores how technical gaps in the investigation and formulation of charges not just weak laws can lead to failure of prosecution.

Moving from the institutional to the legislative or procedural domain, the Cybercrimes Act itself exhibits significant procedural vacuums. For instance, section 45(1) empowers law enforcement, once an ex-parte warrant is obtained, to access computer systems and decode or decrypt any coded or encrypted data, a welcome power in theory.[24] Yet the statute offers little or no procedural detail on how encryption keys should be obtained, preserved, or how the integrity of decrypted data should be maintained. That lack of guidance places both investigators and service providers in an uncertain space, investigators hesitate, service providers are unsure of their legal obligations, and

---

22 Chaman Law Firm, 'Cyber Crime Prosecution Breakthrough Challenges in Nigerian Courts' <https://chamanlawfirm.com/9-cyber-crime-prosecution-breakthrough-ch/> Accessed 2 November 2025.

23 (2021) LCN/15094(CA).

24 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s.45(1).

evidence recovery often flounders.[25] In an era when vast volumes of data are stored on cloud servers or in offshore jurisdictions, Nigeria's legislative silence is even more critical. Although the Act allows for data preservation orders and digital searches, it contains no robust mechanism for accessing information stored beyond Nigeria's borders, no specific procedure for mutual legal assistance tailored to complex cloud-based evidence.[26] This omission gives offenders a significant tactical advantage, especially when they exploit virtual private networks (VPNs), proxy servers or offshore data centres. Consequently, even when domestic law enforcement works hard, they often hit dead ends simply because the relevant data lies outside Nigerian legal reach or the legal path to retrieve it is unclear.

Ultimately, the digital battlefield moves far faster than Nigeria's legislative and institutional response. Offenders adapt rapidly by layering their offences through VPNs, shift their hosting locations offshore, erase digital trails via encryption, or exploit jurisdictional gaps. Without continuous law reform, dedicated technical capability and procedural clarity, prosecutors and investigators risk being perpetually outpaced. Public confidence in cyber-law enforcement is eroded when high-profile arrests are made only for cases to collapse due to evidential or procedural flaws. The gap between swift technological advance and slower legislative evolution remains one of the greatest impediments to Nigeria's ability to prosecute cyber-offences effectively.

4.3.5 Extraterritorial Jurisdiction and International Cooperation Gaps

Cybercrime, by its very nature, transcends borders. An offence may be conceived in Lagos, executed via servers in Amsterdam, and its victims located in New York. Good

---

[25] Adeleke University Law Journal, 'Spate Of Cybercrimes In Nigeria: Evidence Of Gaps In The Legal Frameworks' <https://aulj.adelekeuniversity.edu.ng/index.php/aulj/article/view/13?Utm> Accessed 2 November 2025.

[26] Dayo Akindipe 'Spate Of Cybercrimes In Nigeria: Evidence Of Gaps In The Legal Frameworks' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4918996&utm> Accessed 2 November 2025.

law must recognize that fluidity. The Act attempts to do so under Section 50 of the Cybercrime Act, which states that the Federal High Court of Nigeria shall have jurisdiction to try offences under the Act even if committed outside Nigeria, but only in certain specified circumstances: when the victim is a citizen or resident of Nigeria, or when the alleged offender is physically in Nigeria and has not been extradited.[27] Yet the practical reality is far more challenging. Despite this promising extraterritorial clause, Nigeria's ability to enforce it remains weak. One key obstacle is that while Section 50 provides for jurisdiction, it does not automatically guarantee enforcement or cooperation from other states. The Act also includes Section 51 of the same, which deals on extradition and Section 52 dwelling on mutual legal assistance to bolster cross-border cooperation, but these provisions have limited traction in practice.[28] For example, the Attorney-General may request assistance from foreign states under Section 52(1), even if no bilateral or multilateral treaty exists, but no strong guarantee of timely or effective assistance is built into the statute itself.[29]

In the context of international practice, the gap becomes more visible when compared with instruments such as the Budapest Convention on Cybercrime. That Convention explicitly outlines detailed mechanisms for cross-border data preservation, expedited mutual legal assistance and harmonized jurisdictional rules.[30] Nigeria's legal architecture on paper references these, but the lack of robust treaties, operational agreements and institutional alignment means the practical law-enforcement effects are modest. A recent country-overview report emphasizes that although Nigeria's law grants passive

---

27 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s. 50.

28 Ibid., ss. 51–52.

29 Oyetola M. Atoyebi, SAN, 'Acceding to International Cybersecurity Conventions', <https://www.opinionnigeria.com/acceding-to-international-cybersecurity-conventions-by-oyetola-muyiwa-atoyebi-san/> Accessed 2 November 2025.

30 Budapest Convention on Cybercrime, Art. 22–23, Jurisdiction and Extradition/Mutual Assistance.

extraterritorial jurisdiction and active jurisdiction under Section 50, the requirement of double criminality and weak institutional frameworks often hamper enforcement. Furthermore, when offences exploit offshore servers or jurisdictions with weak cooperation frameworks, the lack of practical data-sharing and asset recovery mechanisms becomes a major disadvantage. Investigators may identify a Nigerian victim and trace an offence to servers in another country, but if the foreign host country does not respond promptly to a mutual legal assistance request or refuses cooperation altogether, the Nigerian prosecution may collapse or never start. Beyond that, the lack of clear frameworks for asset tracing, freezing and repatriation under the Act compounds the problem, while Section 48 allows for forfeiture of proceeds even if domiciled abroad, the enforcement across jurisdiction remains weak.[31]

In short, the Act's extraterritorial jurisdiction and cooperation provisions are aspirational, they set a legal foundation but fall short of guaranteeing operational success. They require institutional capacity, dedicated diplomatic frameworks, technical interoperability, and multinational agreements to function effectively none of which are fully matured in Nigeria's context. Until these supporting systems are in place and fully functional, even the most well-drafted legal provisions risk remaining theoretical.

4.4 COMPARATIVE ANALYSIS OF THE NIGERIAN LEGAL FRAMEWORK ON CYBERCRIME WITH OTHER JURISDICTIONS

A meaningful evaluation of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 requires looking beyond Nigeria's borders to see how other countries structure and enforce their cybercrime laws. Comparing Nigeria's framework with those of the United Kingdom and the United States helps reveal where Nigeria's law is strong, and where it

[31] FE Eboibi 'A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act 2015' <https://delsulawreview.com/wp-content/uploads/2023/07/3.-A-Critical-Exposition-Of-The-Nigerian-Cybercrimes-Prohibition-Prevention-Etc-Act-2015.pdf?Utm> Accessed 2 November 2025.

still falls short. Both the Computer Fraud and Abuse Act (CFAA) in the U.S. and the Computer Misuse Act 1990 (CMA) in the U.K. are long standing statutes that have evolved alongside technology. By examining them, one gains a clearer understanding of what Nigeria has achieved and what still needs reform, particularly in terms of clarity, enforcement, and technological adaptability.

4.4.1 Definitions, Scope, and Coverage

In advanced legal systems, cybercrime laws are drafted with precision, leaving little room for ambiguity. For instance, the UK's Computer Misuse Act 1990 clearly outlines key offences such as unauthorised access to computer material , unauthorised access with intent to commit further offences , and unauthorised modification of data provided in section 1,2 and 3 of the Act respectively. These categories create a clear structure that enables prosecutors and investigators to easily identify and classify offences.

Nigeria's Cybercrime Act 2015, by contrast, attempts a wider but less detailed coverage. It addresses hacking, cyberterrorism, identity theft, and offences against national information infrastructure, while also mandating cooperation from service providers. However, it lacks clarity in defining what constitutes unauthorised access or hacking in all its forms. Scholars such as Omotubora have pointed out that the Act's omission of basic hacking, that is, unauthorised access without an additional offence creates a gap that can frustrate prosecution.[32] Moreover, while jurisdictions like the U.K. and U.S. regularly update their laws to reflect new threats such as cloud-based attacks, cryptocurrency-related frauds, or artificial intelligence misuse, Nigeria's Act remains

[32] A Omotubora, 'Comparative Perspectives on Cybercrime Legislation in Nigeria and the UK – A Case for Revisiting the Hacking Offences under the Nigerian Cybercrime Act 2015', *European Journal of Law and Technology*, Vol. 7, No. 3 (2016),< https://ejlt.org/index.php/ejlt/article/view/524> Accessed 2 November 2025.

relatively static. This rigidity limits its ability to deal with modern realities of cybercrime, where offences evolve faster than legislative reform.[33]

4.4.2 Jurisdiction and Extraterritorial Reach

Cybercrime rarely respects borders, making extraterritorial jurisdiction vital for effective enforcement. The U.S. and U.K. both empower their authorities to prosecute offences committed abroad if those crimes affect domestic systems or citizens. These countries also maintain well-established Mutual Legal Assistance Treaties (MLATs) and real-time data-sharing arrangements with other jurisdictions. The Cybercrime Act 2015 recognizes this need in Sections 50 and 52, granting Nigeria power to prosecute certain offences committed outside its territory.[34] However, the implementation of these provisions remains weak. Challenges such as limited international partnerships, bureaucratic delays, and inadequate coordination among agencies reduce their effectiveness.[35]

In practice, cybercrime investigations often require cooperation from foreign based internet service providers, hosting companies, or financial institutions, something Nigeria still struggles with due to weak legal and diplomatic mechanisms. Unlike countries that have established National Computer Emergency Response Teams (Certs) and international task forces, Nigeria's cooperation frameworks are still developing, making it harder to track and prosecute transnational offenders.

4.4.3 Procedural Powers, Evidence, and Enforcement Infrastructure

Cybercrime investigation requires not only legal provisions but also advanced procedural powers and technical expertise. In the U.K., the Investigatory Powers Act 2016 and the

---

33 Ibid.

34 PT Ortese, 'An Appraisal of the Nigerian Cyber Crimes Law from Comparative Perspective', *Law Journal, pg 31* (2023),< https://www.bsum.edu.ng/journals/law/vol12n1/article4.php> Accessed 2 November 2025.

35 Ifoma Nwafor 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps', *African Journal of Legal Studies, pg 13* (2024),< https://brill.com/view/journals/ajls/16/3/article-p249_3.pdf> Accessed 2 November 2025.

Regulation of Investigatory Powers Act 2000 provide detailed authority for real-time interception, data preservation, and search of electronic devices all under judicial oversight.

While Nigeria's Cybercrime Act contains similar provisions contained in sections 45–49 that authorize search, seizure, and interception, enforcement is often limited by weak forensic infrastructure and a shortage of trained investigators and judges. According to Daudu and Idehen , the Nigerian framework is silent on essential investigatory initiatives and lacks the procedural sophistication seen in advanced systems.[36]

Another major issue lies in digital evidence management. Although Nigeria's Evidence Act recognizes electronic evidence, courts often face difficulties in authenticating or verifying such evidence due to lack of technical expertise and chain-of-custody standards. In the U.K. and U.S., specialized cybercrime courts, forensic laboratories, and trained digital analysts help bridge this gap ,something Nigeria is yet to establish fully.

4.4.4 Penalties, Sanctions, and Deterrence

On paper, Nigeria's penalties for cybercrime are strong. Some offences attract up to ten years of imprisonment and heavy fines.[5] However, enforcement and deterrence depend not only on the severity of penalties but also on the certainty of punishment. In the U.K., for example, penalties under the Computer Misuse Act initially carried lighter sentences but were later strengthened through amendments and consistent enforcement. Research shows that Nigeria's main challenge lies not in punishment but in prosecution. Many cybercrime cases never reach conviction due to procedural gaps or poor evidence. As a

[36] SO Daudu & SO Idehen, 'Legal and Institutional Framework for Combating Cybercrimes in Nigeria'(2024), <https://journals.kwasu.edu.ng/index.php/lexscriptio/article/view/142> Accessed 2 November 2025.

result, potential offenders may not view the system as a credible deterrent.[37] In contrast, the U.S. and U.K. regularly publicize successful prosecutions, sending a strong message that digital crimes have real-world consequences.

4.4.5 Private Sector Cooperation and Service Provider Obligations

Cybercrime prevention thrives on public–private collaboration. In the U.S., the Cybersecurity Information Sharing Act (CISA) 2015 encourages companies to share threat data with government agencies. Similarly, the U.K. has formalized cooperation through initiatives between law enforcement and major tech firms, ensuring early detection and coordinated responses to attacks. Nigeria's Cybercrime Act includes provisions for service provider cooperation and establishes a National Cybersecurity Fund under Section 44, yet the framework remains underdeveloped. There is no clear obligation for mandatory breach reporting or structured information-sharing platforms between the private sector and government.[38] As a result, many cyber incidents go unreported, limiting the ability of law enforcement to detect patterns and prevent larger attacks. For a country with an expanding digital economy, this lack of synergy between public institutions and private entities is a major gap. Modern cyber defence depends not just on law but also on trust, shared responsibility, and real-time communication between stakeholders.

From this comparative analysis, several insights emerge. Nigeria's Cybercrime Act 2015 is comprehensive in concept and covers most core offences, but it lacks the clarity and

---

[37] Olisa Agbakoba, 'Cybercrimes and Cyber Laws in Nigeria: All You Need To Know' <https://www.mondaq.com/nigeria/security/1088292/cybercrimes-and-cyber-laws-in-nigeria-all-you-need-to-know> Accessed 2 November 2025.

[38] Charity Chinedu-Uhuo & Paschal Oguguo Olebara, 'A Comparative Analysis of the Legal Framework on Cybercrime Prevention in Nigeria with the United States of America, Canada and Egypt', *Alex Ekwueme Federal University Law Journal, pg 19* (2024), <https://nigerianjournalsonline.com/index.php/AEFULJ/article/view/5397> Accessed 2 November 2025.

technical depth found in U.S. and U.K. laws. Jurisdictional reach exists in law but falters in execution due to limited cross-border cooperation and data-sharing infrastructure. Procedural mechanisms and forensic capacity are underdeveloped, weakening investigative and prosecutorial success. High penalties exist, yet deterrence remains weak because of poor enforcement and low conviction rates. Finally, collaboration with private sector stakeholders ,a cornerstone of modern cybersecurity frameworks remains insufficient.

Ultimately, Nigeria's law is a robust foundation, but it must evolve to meet the sophistication of contemporary cyber threats. The lessons from mature jurisdictions are clear, success in cybercrime regulation depends as much on institutional capacity, technological investment, and coordinated enforcement as it does on the strength of the law itself.

4.5 CHALLENGES FACED IN COMBATING CYBERCRIME IN NIGERIA

4.5.1 Technical Challenges

Despite the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, Nigeria continues to grapple with significant technical barriers that limit its effectiveness in tackling cyber offences. The most pressing of these challenges is the country's shortage of skilled digital forensics professionals, modern laboratories, and reliable cyber infrastructure. Investigators frequently depend on outdated tools and manual processes that are ill-suited for handling today's sophisticated digital evidence.[39] As a result, many prosecutions collapse in court because prosecutors struggle to establish the authenticity, chain of custody, and integrity of digital exhibits such as IP logs, metadata, encrypted files, or cloud-stored records.

[39] Shuaib Oniye & Abiodun A Kannike, 'Challenges in the Enforcement of Cybercrimes Law in Nigeria: Yahoo Plus as Case Study'< https://kwasuspace.kwasu.edu.ng/handle/123456789/2264> Accessed 2 November 2025.

An investigation on Yahoo-plus revealed that this technical deficit has repeatedly led to failed prosecutions.[40] They observed that in many instances, digital footprints were tampered with or lost before being properly seized, making conviction virtually impossible under the evidentiary standards of the Evidence Act 2011. This reality underscores how technological backwardness can directly undermine the enforcement of even the most robust legal provisions. The problem is compounded by the speed at which cybercrime tactics evolve. Criminals now rely on advanced tools such as end-to-end encryption, blockchain transactions, cryptocurrency mixers, virtual private networks (VPNs), and botnets to conceal their identities and operations.[41] Meanwhile, Nigeria's investigative and legal frameworks have not evolved fast enough to keep pace. A striking illustration occurred in September 2022, when a Wired investigation revealed that an unsecured Amazon S3 data bucket belonging to a Nigerian state health agency had been publicly accessible for months, leaking about 45GB of citizens' personal information.[42] This incident laid bare the government's limited cybersecurity awareness and demonstrated how even public institutions remain vulnerable to basic data-protection failures.

Training and capacity development remain sporadic and inconsistent. A significant number of police officers and prosecutors still lack certification in digital forensics, malware analysis, blockchain tracing, or log interpretation.[43] Consequently, many

---

40 Chaman Law Firm '9 Cyber-Crime Prosecution Breakthrough Challenges in Nigerian Courts',<https://chamanlawfirm.com/9-cyber-crime-prosecution-breakthrough-ch/> Accessed 2 November 2025.

41 AOC Solicitors, 'The Evolving Landscape of Digital Law and Cybercrime in Nigeria' (2025) <https://aocsolicitors.com.ng/the-evolving-landscape-of-digital-law-and-cybercrime-in-nigeria/> Accessed 2 November 2025.

42 Zack Whittaker, 'The Deep Roots of Nigeria's Cybersecurity Problem,'< https://www.wired.com/story/nigeria-cybersecurity-issues/> Accessed 2 November 2025.

43 Professions.ng 'Nigerian Police and Cybercrime: How They Tackle the Issue',(2023) <https://professions.ng/nigerian-police-and-cybercrime/> Accessed 2 November 2025.

investigations continue to mirror traditional policing methods rather than the specialized workflows required for modern cybercrime cases. This gap became visible in the Economic and Financial Crimes Commission's (EFCC) 2024 mass arrest of 792 internet-fraud suspects across Lagos, Port Harcourt, and Abuja. Although the arrests were widely celebrated, investigators soon faced lengthy delays in analyzing seized laptops and mobile phones due to a shortage of certified forensic analysts.[44] The scarcity of modern forensic laboratories and secure evidence storage systems further weakens investigative efficiency. Establishing and maintaining such facilities require sustained investment, yet cybersecurity budgets in Nigeria remain thin and inconsistent.[45] Many agencies therefore depend on external consultants or foreign laboratories for forensic support, a dependency that not only slows prosecution but also raises concerns about data privacy and the integrity of digital evidence.

In essence, these technical deficiencies expose the fragility of Nigeria's cyber-enforcement system. Without technological competence, the best of laws remain ineffective against the increasingly sophisticated architecture of online crime.

4.5.2 Operational Challenges

Beyond the technical domain, Nigeria faces deep rooted operational challenges that hinder the effective enforcement of its cybercrime laws. Chief among these is institutional fragmentation. Several agencies including the EFCC, the Nigerian Police Force Cybercrime Unit, the National Information Technology Development Agency (NITDA), and various sectoral regulators exercise overlapping mandates, often without a

---

[44] The Guardian Nigeria, '792 Arrested as EFCC Gets Tough with Cryptocurrency Fraud Syndicate'(2024)<https://guardian.ng/news/nigeria/metro/792-arrested-as-efcc-gets-tough-with-cryptocurrency-fraud-syndicate/> Accessed 2 November 2025.

[45] Mansu Yau 'Competency of Police Investigators on the Application of Digital Forensics in Cybercrime Investigation in Jigawa State Police Command,Nigeria' <https://globalresearchnetwork.us/index.php/ajshr/article/view/3657?Utm> Accessed 2 November 2025.

unified operational framework.[46] This duplication leads to turf rivalries, inconsistent investigations, and poor information sharing, ultimately weakening national response capacity.

In 2024, Lagos Chief Judge Justice Kazeem Alogba publicly cautioned that assigning exclusive cybercrime jurisdiction to the Federal High Court had created serious enforcement bottlenecks. He urged for limited jurisdictional empowerment of state courts to handle less-complex cybercrime matters, thereby reducing congestion and accelerating trials.[47] His observation aptly highlights the structural disconnect between legislative design and practical enforcement. Procedural delays in the courts further aggravate the situation. Cybercrime evidence is extremely time sensitive, digital logs expire, online accounts get deleted, and data can be easily overwritten. Yet Nigeria has no fast track cybercrime divisions or courts.[48] The result is that prosecutions linger for years, weakening digital evidence and discouraging victims from pursuing justice.

Another major limitation lies in international cooperation. While sections 50 and 51 of the Cybercrimes Act extend jurisdiction extraterritoriality and call for cross-border collaboration, the actual execution of mutual legal assistance treaties remains cumbersome.[49] Obtaining foreign hosted evidence for example, from U.S. or European internet service providers often takes months, sometimes years. This problem was evident in the EFCC's 2024 operation against an international romance scam syndicate,

---

46 IF Omonayin, 'Legal Challenges in Combating Cybercrime in Nigeria: Regulations versus Enforcement'(2025) <https://recordoflaw.in/legal-challenges-in-combatting-cybercrime-in-nigeria-regulations-versus-enforcement/> Accessed 2 November 2025.

47 Victor Alogba, 'Federal Courts Can't Handle Cybercrime Cases Alone, Says Lagos Chief Judge,' The Cable (25 Sept 2024)< https://www.thecable.ng/federal-courts-cant-handle-cybercrime-cases-alone-says-lagos-chief-judge/> Accessed 2 November 2025.

48 Ibid.

49 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 50-51

where investigators struggled to trace cryptocurrency trails across foreign exchanges that failed to respond promptly to Nigerian requests.[50]

Under-reporting of offences adds another layer of difficulty. Many victims of online fraud, identity theft, or sextortion choose silence due to shame, limited awareness, or distrust of law enforcement.[51] According to the EFCC, Nigeria loses over US $500 million annually to cybercrime, yet only a fraction of victims ever file formal complaints.[52] This chronic under-reporting deprives authorities of valuable intelligence that could enhance preventive and investigative strategies.

Equally troubling is the perception of selective or politically motivated enforcement. In May 2024, investigative journalist Daniel Ojukwu was arrested under section 24 of the Cybercrimes Act, sparking public outrage and international condemnation. The Associated Press reported that such incidents reinforce fears that the law is being weaponized against dissent rather than used to ensure justice.[53] When citizens perceive cybercrime legislation as a political instrument, public trust erodes, and cooperation with cyber-authorities diminishes, a development that weakens collective security.

Finally, persistent funding shortfalls continue to undermine progress. Cybercrime enforcement requires continuous investment in digital infrastructure, forensic software, secure data storage, and staff training. Yet most agencies depend on sporadic project

---

50 Ibid.

51 U F Nzeakor, 'Why Do Cyber-Crime Victims Fail to Report Their Victimisation Experiences to the Police? A Survey of the Factors of Poor Attitude towards Reporting Cyber-Crime Victimisation in Nigeria' (2023) ResearchGate <https://www.researchgate.net/publication/375090505_WHY_DO_CYBERCRIME_VICTIMS_FAIL_TO_REPORT_THEIR_VICTIMIZATION_EXPERIENCES_TO_THE_POLICE_A_SURVEY_OF-THE-FACTORS-OF-POOR-ATTITUDE-TOWARDS-REPORTING-CYBERCRIME-VICTIMIZATION-IN-NIGERIA> Accessed 2 November 2025.

52 Punch Newspapers, 'Nigeria Loses Over $500m to Cybercrime Annually — EFCC Chair' (13 June 2024) https://punchng.com/nigeria-loses-over-500m-to-cybercrime-annually-efcc-chair/ Accessed 2 November 2025.

53 Associated Press, 'Nigerian Journalist's Arrest Last Week Triggers Criticism of Worsening Press Freedoms' (6 May 2024) < https://apnews.com/article/08b6835eb9d7002f585be54674eb82e9> Accessed 2 November 2025.

funding or external donor grants.[54] Without consistent financial support, legislative innovation risks remaining symbolic, with little impact on the ground..

4.6 CONCLUSION

Taken together, these technical and operational weaknesses explain the enduring enforcement gap despite Nigeria's comprehensive legal framework. Scholars and practitioners alike agree that the nation's problem is not a lack of legislation but a lack of institutional capacity and inter-agency coordination to transform law into deterrence. To bridge this gap, Nigeria must invest in specialized cyber-crime courts, harmonised coordination mechanisms, strong international partnerships, and a public-sector culture that prioritizes cybersecurity literacy at every level of governance. Only through such systemic transformation can the Cybercrimes Act 2015 achieve its full potential in safeguarding Nigeria's digital future.

[54] S C Nzenwa, 'An Appraisal of the Legal Framework for Cybercrimes in Nigeria'*African Journal of Criminal Law and Jurisprudence* (2025) <https://journals.ezenwaohaetorc.org/index.php/AFJCLJ/article/viewFile/3266/3414> Accessed 2 November 2025.

CHAPTER FIVE

RECOMMENDATIONS AND CONCLUSION

5.1 SUMMARY OF FINDINGS

The study establishes that Nigeria has developed a broad and seemingly comprehensive statutory architecture for combating cybercrime. At the centre of this framework is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended, supported by the Advance Fee Fraud Act, the Economic and Financial Crimes Commission (Establishment) Act, and the Money Laundering (Prevention and Prohibition) Act 2022. Collectively, these laws outline major cyber offences, prescribe penalties, confer extraterritorial jurisdiction, and recognize the cross-border nature of digital criminality. In terms of legislative ambition, the Nigerian framework is comparable to those of more advanced jurisdictions.

However, the findings reveal that the operational effectiveness of these laws is significantly weakened by persistent implementation deficits. A major challenge is the acute shortage of specialized forensic capacity within enforcement institutions. The study shows that Nigeria lacks adequate numbers of certified cyber investigators, functional digital forensic laboratories, and modern investigative tools. The result is frequent evidentiary failures, including compromised chain-of-custody processes, rejected electronic evidence, and collapsed prosecutions. These technical shortcomings undermine the deterrent effect expected from the statutory penalties.

Institutional fragmentation also emerged as a central problem. The mandates of key enforcement bodies such as the EFCC, the Nigeria Police Force cyber units, NITDA, NFIU, and other regulators often overlap, creating turf rivalries, duplication of effort, and an absence of sustained coordination. The study further identifies that Nigeria lacks a

clearly designated national coordinating authority for cybercrime enforcement, resulting in inconsistent strategic direction and inefficient deployment of available resources.

The judiciary is another pressure point. The exclusive jurisdiction of the Federal High Court over cybercrime matters has produced delays, backlogs, and bottlenecks, especially when time sensitive digital evidence is involved. Procedural limitations within the justice system also contribute to weakened prosecutions, as many judges and prosecutors lack adequate training in the handling, interpretation, and admissibility of digital evidence.

From a legislative perspective, the study notes substantive gaps and ambiguities within the Cybercrimes Act itself. Key definitions such as those relating to unauthorized access, system interference, and digital manipulation are imprecise, leaving significant interpretative room and complicating prosecutions. The Act does not expressly address several emerging cyber threats, including deepfakes, AI-driven criminal activity, certain cryptocurrency based frauds, and botnet related offences. These omissions create exploitable loopholes for technologically sophisticated offenders. The National Cybersecurity Fund, intended as a sustainable financing mechanism for cybercrime enforcement, is found to be administratively opaque and operationally inconsistent, with unclear procedures for levy collection and oversight.

The findings also underscore weak public-private collaboration. Mandatory breach reporting is limited, information sharing channels between government agencies and private entities remain informal or underutilized, and victims often decline to report cyber incidents due to fear, stigma, or lack of confidence in the system. Such under-reporting erodes the intelligence base required for early detection and coordinated responses.

Finally, the study highlights the inadequacies of international cooperation mechanisms. Delays in mutual legal assistance processes, challenges in obtaining data stored abroad,

and the absence of formalized partnerships with major technology and cryptocurrency companies significantly hinder Nigeria's ability to prosecute transnational cybercrime.

Overall, the findings show that Nigeria's legal regime, while robust on paper, is weakened by institutional, technical, procedural, and operational shortcomings. Without addressing these structural barriers, the full potential of the statutory framework cannot be realized, and emerging digital threats will continue to outpace the nation's response capacity.

5.2 RECOMMENDATION

The findings of this study clearly indicate that Nigeria's statutory framework for combating cybercrime is extensive, yet its practical effectiveness is severely constrained by implementation deficiencies, institutional fragmentation, and limited technical capacity. To address these challenges, several interrelated reforms are essential. Legislative review and targeted amendment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended are imperative to align the law with contemporary technological realities. The Act requires clarification of core concepts such as unauthorized access, system interference, and digital fraud, while emerging forms of cybercrime, including deepfakes, AI-enabled manipulation, cryptocurrency laundering schemes, and botnet provisioning, must be expressly criminalized. Equally important is the establishment of clear legal parameters for investigative powers, accompanied by safeguards to protect fundamental rights, thereby ensuring that enforcement does not compromise constitutional guarantees.

Institutional realignment is equally crucial. The current overlapping mandates of enforcement agencies, including the EFCC, police cyber units, NITDA, NFIU, and sectoral regulators, hinder coordinated action and dilute operational efficiency. Creating a single, accountable coordinating authority for national cybercrime management would

streamline operations, enhance inter-agency cooperation, and ensure the transparent administration of the National Cybersecurity Fund. This institutional consolidation would address turf disputes, duplication of effort, and administrative opacity, thereby fostering more effective enforcement.

Capacity building and infrastructural development must form a core part of Nigeria's cybercrime strategy. Investment in regional digital forensic laboratories, accredited evidence storage facilities, and ongoing professional training for investigators, prosecutors, and judges in advanced digital forensic techniques and blockchain analysis is necessary to close current technical gaps. Where domestic capacity remains insufficient, regulated cooperation with trusted foreign laboratories may serve as an interim measure, provided that data integrity and privacy are safeguarded.

Judicial and procedural reforms are also required to address court congestion and evidentiary challenges. Empowering lower courts to adjudicate less complex cyber offences, establishing specialized cybercrime benches or fast-track dockets for time-sensitive digital evidence, and issuing prosecutorial guidelines for evidence preservation and chain-of-custody management will reduce delays and strengthen the likelihood of successful prosecutions.

Enhancing public-private cooperation is critical for timely detection and prevention. Formalizing mandatory breach reporting, creating secure platforms for sharing indicators of compromise, and providing legal safe harbours for good-faith reporting will encourage collaboration between government agencies and private sector actors. At the community level, simplified reporting portals, victim support services, and restitution mechanisms are necessary to mitigate chronic under-reporting and ensure a steady flow of actionable intelligence.

Finally, international cooperation and sustainable financing must be prioritized. Streamlining Mutual Legal Assistance Treaty processes, negotiating bilateral and multilateral agreements, and formalizing collaboration with major cloud and cryptocurrency service providers will facilitate timely access to foreign-hosted evidence. Sustainable funding mechanisms, governed by transparent collection rules, independent auditing, and parliamentary reporting, will ensure consistent investment in infrastructure, human capital, and public awareness initiatives essential for an effective cybercrime response.

5.3 CONCLUSION

In conclusion, the study demonstrates that while Nigeria's legal framework for combating cybercrime is conceptually comprehensive and broadly aligned with international standards, its effectiveness is significantly undermined by structural, technical, and procedural deficiencies. The primary obstacles are not legislative absence but gaps in implementation, institutional coordination, technical capacity, judicial processing, public-private engagement, and international collaboration. These weaknesses collectively reduce the deterrent effect of the law, lead to avoidable evidentiary failures, and allow emerging cyber threats to exploit systemic vulnerabilities.

Addressing these challenges requires a holistic approach that integrates legislative amendment, institutional consolidation, technical capacity building, judicial reform, stakeholder engagement, and sustainable financing. By implementing these reforms, Nigeria can transform its statutory framework into a functional and dynamic system capable of deterring cybercrime, safeguarding citizens' rights, fostering investor confidence, and positioning the nation as a credible participant in the global digital economy. The findings of this study provide both the empirical diagnosis and policy road map necessary for a coherent, future-ready national strategy to combat cybercrime.

BIBLIOGRAPHY

Books

Ajayi OA, *Internet Technologies and Cybersecurity Law in Nigeria* (Malthouse Press, Lagos, 2024) 45

Iorliam A, *Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime* (SpringerBriefs in Cybersecurity, Cham, 2019) 12–30

Nwafor IE, *Cybercrime and the Law: Issues and Developments in Nigeria* (Centre for Law and Development Studies, Enugu, 2022) 81

Sibe RT and Kaunert C, *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria* (Springer, Cham, 2024) 95

Journal Articles

Abubakar A, 'Cybercrime in Nigeria: A Socio-Legal Analysis with Focus on Jigawa State' *Global Journal of Arts, Humanities and Social Sciences* Vol. 6 No. 10 (2018) 24–33

Adejumo AD and Oyeniyi KO, 'Cybercrime and its Effect on Nation Identity Image: Pragmatic Evidence from Nigeria' *PJMI* (2025)

Adeleke A and others, 'A Universal Definition of Cybercrime: The Consequences of Incoherence' *Adeleke University Law Journal* Vol. 1 (2020)

Afolabi MB and Esoso AJ, 'The Role of Youths in Cybercrime in Nigeria' *South Global Journal of Humanities and Development Studies* Vol. 2 No. 1 (2021)

Aknai NK, 'Information and Communication Technology: An Evaluation of Cyber Crimes Laws in Nigeria' (2024)

Apeloko OD and Chiamaka CS, 'Impacts of Cyber Crimes on the Image of Nigeria in the International Community: *A Case of the Perceptions of Ghanaians'* (2025)

Ashiru NI, 'Identifying Phishing as a Form of Cybercrime in Nigeria' (2025)

Ayesh Perera, ‘Routine Activities Theory: Definition & Examples’ (2025).

Babafemi Tomilehim, ‘An Appraisal of the Legal Framework of Cybercrime in Nigeria’ (2025).

Bello M and Griffiths M, ‘Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable are Law Enforcement Agencies?’ (2024)

Clancy, Ryan, ‘Password Sniffing in Ethical Hacking’ (2025).

Eboibi E, ‘A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015’ *Delta State University Law Review* (2023)

Egbo C, ‘A Critical Analysis of the Law Regulating Cybercrimes in Nigeria’ (2022)

Garuba J, ‘An Approach to Cybercrime Issues in Dandume Local Government Area of Katsina State Nigeria’ (2025)

Imam Abdulbasit, ‘Nigeria’s Foreign Relations and Soft Power Diplomacy’ *SSRN* (2025)

Jamo IA, ‘The EFCC and Anti-Corruption Crusade in Nigeria: Success and Challenges’ *Gusau International Journal of Management and Social Sciences* (2021) 102–120

Obasohan JO and Akpata R, ‘Cybercrime and Ritualism: An Analysis Under the Criminal Code’ (2025)

Ogbotor MS, ‘Effectiveness of Anti-Money Laundering Regulations in the Nigerian Banking Sector’ *Journal of Business and African Economy* (2025) 1–15

Olivia OE, ‘Examining the Effect of the Elevated Rate of Cybercrime on the Growth and Sustainable Development of Nigeria’s Economy’ (2025)

Onadeko OA and Afolayan AF, ‘A Critical Appraisal of the Cybercrimes Act 2015 in Nigeria’ *ISRCL* (2018)

Paul Ohm, ‘Legal Issues Surrounding Monitoring During Network Research’ (2007).

Udoinyang N & David A, ‘Relationship Between Cybercrime and the Nigerian Economy: Causes, Implications and the Path Forward’ *Journal of Financial and Business Management Studies* (2024)

Yinusa MA & Sulaiman AL, ‘Cybercrime and Nigeria’s External Image: A Critical Assessment’ (2018)

Uzoka Ngozi & Umejiaku N, ‘Cybercrime and Digital Transaction Laws in Nigeria: A Review’ (2025)

Websites/Online Sources

Business Day Nigeria, ‘Scandal Rocks EFCC as Officers Disappear with Seized Gold, $30,000’ (2025). <https://businessday.ng/news/article/scandal-rocks-efcc-as-officers-disappear-with-seized-gold-30000/>accessed 2nd November 2025.

EFCC, multiple case reports (2023–2025). <https://www.efcc.gov.ng/efcc/news-and-information/news-release/11079-court-jails-man-one-year-for-internet-fraud-in-lagos>accessed 2nd November 2025.

Guardian Nigeria, multiple reports (2025). <https://guardian.ng/news/nigeria/metro/three-convicted-of-internet-fraud-sentenced-to-90-months-imprisonment/>accessed 2nd November 2025.

Hushpuppi — Wikipedia (2025). <https://en.wikipedia.org/wiki/Hushpuppi>accessed 2nd November 2025.

Premium Times, ‘EFCC Traces $30,000 to Suspected Internet Fraudster’ (2025). <https://www.premiumtimesng.com/news/more-news/792585-efcc-traces-30000-to-suspected-internet-fraudster.html>accessed 2nd November 2025.

Punch Newspaper, ‘How Authorities Use Cybercrime Act to Target Journalists’ (2025). <https://punchng.com/how-nigerian-authorities-use-cybercrime-act-to-harass-detain-journalists-activists/>accessed 2nd November 2025.

The Cable, ‘Federal Courts Can’t Handle Cybercrime Cases Alone’ (2025). <https://www.thecable.ng/federal-courts-cant-handle-cybercrime-cases-alone-says-lagos-chief-judge/>accessed 2nd November 2025.