AN ANALYSIS OF THE LEGAL FRAMEWORK ON CYBERCRIME IN NIGERIA

Prof. Theresa Uzoamaka Akpoghome and Dr. Nkechinyere Huomachi Worluh-Okolie*

A. Abstract

This paper examines Nigeria's legal framework on cybercrime to assess its adequacy in addressing emerging threats. It analyses the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, the 2024 Amendment, and related statutes. Adopting a doctrinal approach, the study engages statutory provisions, case law, and scholarly works. Findings reveal that while Nigeria's legal framework represents a significant step toward combating cybercrime, enforcement is hampered by evolving technological threats, jurisdictional complexities, and low public awareness. The study recommends increased funding and training for enforcement agencies, judicial capacity building in digital evidence, and stronger safeguards for citizens' digital rights. It concludes that Nigeria's framework, though progressive in scope, requires robust implementation strategies and international cooperation to effectively secure its cyberspace and build public trust.

Keywords: Cybercrime, Cyber-security, Regulation, Enforcement, Nigeria

B. Introduction

The rapid advancement of information and communication technologies has transformed social, economic, and political interactions worldwide. In Nigeria, the growing reliance on digital platforms for business transactions, communication, and governance has created new opportunities for innovation but has equally exposed the nation to the risks of cybercrime.[1] Offenses such as internet fraud, identity theft, Phishing, child pornography, intercepting electronic communication, cyber-stalking, and cyber-terrorism now threaten not only individual rights but also national security and economic development.[2] The country's notoriety for online scams, popularly referred to as "Yahoo Yahoo," has further

* Akpoghome, Theresa U, Professor, Faculty of Law, Benson Idahosa University, Benin City. Email: takpoghome@biu.edu.ng, teremajor@gmail.co. Ph: 08065436545, 08056317472.

Worluh-Okolie, Nkechinyere Huomachi, Senior Lecturer, Faculty of Law, Benson Idahosa University, Benin City. Email: nworluh-okolie@biu.edu.ng, nkechiworluhokolie@gmail.com. Ph: 08062284449. ORCID ID: https://orcid.org/0009-0007-6794-7468

1 *B.A. Omodunbi, O. M Odiase, and A. O Esan*, "Cybercrimes in Nigeria: Analysis, Detection and Prevention" *Journal of Engineering and Technology* (2016) Vol. 1, Issues I, September 37 -41. <https://www.researchgate.net accessed on 30th August 2025.

2 *Ibid*.

attracted international attention, tarnishing Nigeria's global image and raising concerns about the adequacy of its legal and institutional frameworks for combating cybercrime.[3]

To respond to these threats, Nigeria enacted the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024,[4] which remains the first and most comprehensive legislation on cybercrime in the country.[5] The Act criminalizes a wide range of offenses including hacking, cyber-stalking, child pornography, and financial fraud, while also imposing obligations on institutions such as banks and internet service providers to aid enforcement.[6] Alongside this statute, other laws such as the Nigeria Data Protection Act (NDPA), the Economic and Financial Crimes Commission (EFCC) Act,[7] the Nigerian Communications Commission (NCC) Act,[8] and the Evidence Act, 2011[9] provide additional legal support for the prosecution of cyber-related crimes.

Despite these efforts, challenges of enforcement, weak institutional capacity, jurisdictional complexities, and conflicts between state surveillance and the protection of fundamental rights continue to undermine the effectiveness of Nigeria's response.

This study therefore aims to critically analyse the Nigerian legal framework on cybercrime with a view to assessing its adequacy in addressing current and emerging threats. It adopts a doctrinal methodology, relying on statutory interpretation, judicial decisions, and comparative analysis with international frameworks such as the Budapest Convention on Cybercrime and regional responses like South Africa's Cybercrimes Act, 2020. The study seeks to highlight the strengths and weaknesses of Nigeria's existing framework, examine enforcement challenges, and propose reforms that would enhance the effectiveness of the law while safeguarding digital rights.

The significance of this research lies in its contribution to the growing body of scholarship on cyber security law in Africa. By identifying gaps in Nigeria's legal regime and

3 EFCC (Media and Publicity), "Court Jails Yahoo Yahoo Kingpin, One Other in Calabar" (June 27, 2019)
https://www.efcc.gov.ng/efcc/news-and-information/news-release/4486-court-jails-yahoo-yahoo-kingpin-one-other-in-calabar accessed on 30th August 2025.

4 Available at: https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf accessed on 30th August 2025.

5 As laudable as the Act is, the Act has failed to totally arrest the ugly trend because of some gap or lacuna in the Act and also due to so many other factors that exacerbate cybercrime in Nigeria. See: Umejiaku Nneka Obiamaka and Anyaegbu Mercy Ifeyinwa, "Legal Framework For The Enforcement Of Cyber Law And Cyber Ethics In Nigeria"(2016) (15) (10) *International Journal of Computers and Technology*, 2277 – 3061.

6 See sections 8 – 18 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.

7 Cap. E1, Laws of the Federation of Nigeria, 2010.

8 Available at: https://www.ncc.gov.ng/sites/default/files/2024-12/Legislation-Nigerian_Communications_Act_2003.pdf accessed on 30th August 2025.

9 Available at: https://archive.gazettes.africa/archive/ng/2011/ng-government-gazette-dated-2011-06-21-no-80.pdf accessed on 30th August 2025.

suggesting reforms, the paper provides valuable insights for policymakers, law enforcement agencies, legal practitioners, and scholars. Furthermore, the findings will be of practical importance to the judiciary in adjudicating cybercrime cases, as well as to civil society in advocating for stronger safeguards against online abuses.

For clarity of analysis, this paper is divided into six sections. Following this introduction, the second section clarifies key concepts such as cybercrime, cyber security, cyberspace, and digital rights, which are essential for understanding the scope of the discussion. The third section examines the substantive provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, alongside other relevant legislation. The fourth section considers the institutional framework for combating cybercrime in Nigeria, with emphasis on the roles of the EFCC, NCC, and the Office of the National Security Adviser. The fifth section discusses the major challenges to enforcement and evaluates Nigeria's compliance with international standards, drawing comparative insights from other jurisdictions. The sixth section presents recommendations for reform, while the final section offers the conclusion of the paper.

C. Clarification of Terms

In order to properly analyse the Nigerian legal framework on cybercrime, it is necessary to clarify certain key concepts that are central to this study. The terms cybercrime, cybersecurity, cyberspace, and digital rights are often used interchangeably in both scholarly and policy discourses, yet they carry distinct meanings that must be carefully delineated.

I. Cyber crime

Section 2 of the Criminal Code Act of Nigeria defines crime as an act or omission which renders the person doing the act or making the omission liable to punishment under the Code or under any other Act.[10] The word cyber-crime is a hybrid word. It is made of "cyber" and "crime". The Commonwealth Organisation,[11] states that cyber-crime includes not only crimes against computer systems (such as hacking, denial of service attacks and the set-up of botnets) but also traditional crimes committed on electronic networks (e.g. fraud via phishing and spam; illegal Internet-based trade in drugs, protected species and arms) and illegal content published electronically, (such as child sexual abuse material).

10 Criminal Code Act, S. 2.

11 Commonwealth Organisation, *Cybercrime* (Commonwealth Secretariat 2015). Cited in: Olusola Joshua Olujobi, "Analysis of the Legal Frameworks for Combating Cyber Crimes: A Tool for Economic Development in Nigeria" (2021) (2) (1) *KWASU Law Journal*; pg. 1 – 27. https://www.researchgate.net/publication/361224574_Analysis_of_the_Legal_Frameworks_for_Combating_Cyber_Crimes_A_Tool_for_Economic_Development_in_Nigeria accessed on 30th August 2025.

The word cyber-crime refers broadly to criminal activities carried out using computers, networks, or digital devices. Because our society is evolving towards an information society where communication occurs in cyberspace, cybercrime is now a global phenomenon. Cybercrime has the potential to significantly influence our lives, society, and economy.[12] It encompasses two broad categories:

(a) Crimes that are unique to cyberspace, such as hacking, denial-of-service attacks, and the spread of malicious software; and
(b) Traditional crimes that are facilitated through digital platforms, including fraud, identity theft, child pornography, and money laundering.

Cybercrime also includes nonmonetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.[13] The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 adopts a similarly wide definition, capturing offenses that exploit information and communication technologies (ICTs) to harm individuals, organizations, or the state.

II. Cyber security

Cyber security is the body of practices, technologies, and legal safeguards designed to protect computer systems, networks, and data from unauthorized access, disruption, or destruction.[14] While cybercrime focuses on unlawful acts, cyber security emphasizes protective and preventive measures. Effective cyber security frameworks combine legal, institutional, and technical mechanisms to ensure resilience against cyber threats.

Cyber security is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.[15] Cyber security laws vary a lot from country to country and jurisdiction to jurisdiction. Penalties depend on the nature of offence, and range from a fine to imprisonment.[16]

12 *Josephine Uba,* "Cybercrimes and Cyber Laws in Nigeria: All You Need to Know" (7 July 2021) https://www.mondaq.com/nigeria/security/1088292/cybercrimes-and-cyber-laws-in-nigeria-all-you-need-to-know accessed on 30th August 2025.

13 "The Legal Framework for Cyber Crimes in Nigeria" https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 30th August 2025.

14 *K. Dasshora*, 'Cybercrime in the Society: Problems and Preventions,' (2011), 3(1), *Journal of Alternative Perspectives in the Social Sciences*, 240–259.

15 *D. Craigen and 2 Ors*, "Defining Cybersecurity" (2014) (4) (10) *Technology Innovation Management Review; 13–21.*

16 Uba (n. 11).

III. Cyberspace

Cyberspace refers to the virtual environment created by interconnected digital technologies where communication, transactions, and interactions take place. Unlike traditional physical spaces, cyberspace is borderless, which creates jurisdictional complexities in the enforcement of cybercrime laws.[17] This feature explains why international cooperation is vital in combating cybercrime, as offenses often involve actors and victims in multiple jurisdictions.[18]

IV. Digital Rights

Digital Rights denote the application of human rights principles such as privacy, freedom of expression, and access to information in the digital environment.[19] Legal responses to cybercrime must therefore strike a delicate balance between protecting state security and individual rights online. Excessive surveillance powers or restrictive regulations, though aimed at combating cybercrime, may risk infringing upon fundamental freedoms guaranteed under the Nigerian Constitution and international human rights law.

V. Cyber Law

Cyber law acts as a shield over cyberspace, preventing cybercrime from occurring. The government is committed to developing and enforcing regulations to combat illicit online activities.[20] The "Cybercrimes (Prohibition and Prevention) Act, 2015" has a significant impact on cyber law in Nigeria. This Act creates a comprehensive legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish cybercrime.[21] The Act also encourages cyber security and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights, as well as the protection of important national information infrastructure.[22]

17 *O. J. Olujobi, and T. O. Jolaosho*, "Strategies for Combating the Crimes of Money Laundering and Terrorism Financing in Nigeria: The Need for A Paradigm Shift" (2019) (1) (10) *University of Ibadan Journal of Private and Business law,* 27–64.

18 *F. M. Opebiyi*, "Protecting the Interest of Buyers in Online Contracts of Sale in Nigeria: Making a case for Legislative Intervention" (2018) (1) *Elizade University Law Journal*, 222.

19 *Umejiaku Nneka Obiamaka and Anyaegbu Mercy Ifeyinwa*, "Legal Framework For The Enforcement Of Cyber Law And Cyber Ethics In Nigeria" (2016) (15) (10) *International Journal of Computers and Technology*, 2277 – 3061.

20 Uba (n. 11).

21 *Ibid*.

22 *Ibid*.

D. The Legal Framework on Cybercrime in Nigeria

I. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024

The Cybercrime (Prohibition, Prevention, etc.) Act stands as the central pillar of Nigeria's legislative response to cyber-related offenses. First enacted in 2015 and subsequently amended in 2024,[23] the Act establishes a comprehensive framework for addressing the diverse manifestations of cybercrime recognized under Nigerian law. It provides a unified and functional system for the prevention, detection, investigation, prosecution, and punishment of cyber offenses, thereby strengthening regulatory and enforcement mechanisms within the country.[24]

The 2024 amendments introduced some form of institutionalized response by establishing National Computer Emergency Response Team (ngCERT) and Security Operation Centres (SOCs) to respond to cyber-attacks.[25] The two establishments are to work in synergy. The amended Act placed the responsibility of establishing and coordinating these centres on the office of the National Security Adviser (ONSA).

As a result, it creates a cohesive, efficient, and regulatory system in Nigeria for the prevention, investigation, identification, prosecution, and punishment of cybercrime and other cyber-related offenses. The Act is Nigeria's first comprehensive legislation on cybercrime. It criminalizes offenses such as: It empowers the National Security Adviser (NSA) to coordinate cyber security programs and the Office of the National Security Adviser (ONSA) to enforce compliance. Internet Service Providers (ISPs) are mandated to retain traffic data and cooperate with law enforcement.

Furthermore, the Amended Act mandates that financial institutions must verify the identity of their customers conducting electronic financial transactions by presenting their National Identification Number (NIN) issued by the National Identity Management Commission (NIMC), along with other valid documents bearing their names, before being issued ATM cards, credit cards, debit cards, or similar electronic devices. Under the Principal Act, verification was limited to documents with the customer's name, address, and other information deemed relevant by the Institution.[26]

23 The amendment addresses gaps in the original 2015 act, broadens the scope of offenses, and enhances the nation's capacity to address cybercrime.

24 "The Legal Framework for Cyber Crimes in Nigeria" https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 30th August 2025.

25 *Shettima Mustapha, Shehu Usman Ali and Adama Asingar Yusuf*, "Legal And Institutional Framework For Cyber Security In Nigeria: An Appraisal" (2025) Volume 10, Issue 6 *International Journal of Diplomacy, Legal & International Studies*, PP 1–8, available at: https://www.arcnjournals.org/images/4272-1453-54-1061-1.pdf accessed on 30th August 2025.

26 "The Legal Framework for Cyber Crimes in Nigeria" https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 10th September 2025.

Major offenses and penalties:

The Act addresses a wide array of cyber-related offenses

i. Cyber-terrorism: Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.[27] While Section 18 covers cyber-terrorism broadly, the Act does not expressly mention critical national information infrastructure in the provision itself. However, Part II of the Act does address protective measures for Critical National Information Infrastructure, focusing on safeguarding such assets rather than prescribing penalties for attacks against them.[28]
ii. Illegal access: Section 6 (1) of the Cybercrime Act, makes it an offense for any person to intentionally access, without authorization or in excess of authorization, a computer system or network, especially for fraudulent purposes. It prohibits unauthorized access to a computer system or network either in whole or in part. The offense covers access with intent for fraudulent purposes or to obtain data vital to national security. The penalty for this offense is imprisonment for a term of not less than two years or a fine of not less than 5 million Naira, or both. If committed with the intent to obtain confidential information such as computer data, commercial or industrial secrets, the punishment increases to imprisonment of not less than three years or a fine not less than 7 million Naira, or both. Section 6(4) also covers trafficking in passwords or access information which affects interests inside or outside Nigeria, punishable by imprisonment of up to five years or a fine, or both.[29]
iii. Computer-related forgery and fraud: These offenses involve altering, deleting, or inputting data to create inauthentic information or causing financial loss through electronic messages.[30] This offense occurs when a person knowingly accesses a computer or network and inputs, alters, deletes, or suppresses data resulting in inauthentic data meant to be considered genuine. The penalty on conviction is imprisonment for not less than three years or a fine of not less than 7 million Naira, or both. If the fraud involves sending electronic messages with intent to deceive and cause damage or loss, the penalty increases to imprisonment of not less than five years or a fine of not less

27 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 18 (1).

28 *Nuleera Ambrose Duson and Sunny D James*, "Cyber terrorism and the Protection of Critical Information Infrastructure in Nigeria: A Legal Assessment" (2020) 8 (3) *International Journal of Innovative Legal & Political Studies;* 25 -36.

29 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 6 (1) – (4).

30 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 13.

than 10 million Naira, or both.[31] The Act criminalizes not only direct data manipulation but also the use of electronic messages for fraudulent misrepresentation.[32] These provisions aim to deter electronic fraud and forgery affecting financial transactions, data integrity, and trust in digital communications.[33]

iv. Identity theft and impersonation: Fraudulently using or impersonating another person's identity (dead or alive) information to gain an advantage or obtain property of interest in property or cause harm or disadvantage to the person being impersonated is a criminal offense punishable by imprisonment for not less than three years or a fine of not less than 7 million Naira, or both.[34]

v. Cyberstalking: This is prohibited under the Cybercrime (Prohibition, Prevention, Etc.) (Amendment) Act, 2024 in Nigeria, specifically addressed in Section 24 of the Act. It criminalizes sending grossly offensive, false, or pornographic messages with the intent to cause annoyance, intimidation, or fear to the recipient. The 2024 amendment was made following a judgment by the ECOWAS Court of Justice in March 2022, which ruled that the original Section 24 of the 2015 Cybercrime Act was vague, arbitrary, and repressive. The ECOWAS Court found the original provision violated Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the International Covenant on Civil and Political Rights concerning freedom of expression. The Court ordered Nigeria to amend Section 24 to align with human rights obligations.[35]

Although the 2024 amendment narrowed the definition of cyberstalking, the provision remains broad and has been criticized for continued misuse by Nigerian authorities to harass and intimidate journalists, activists, bloggers, and social media users exercising their rights. Human rights groups like SERAP have challenged the amended law at the ECOWAS Court, arguing it still disproportionately limits free speech and public

31 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 14.

32 *Olanrewaju Adesola Onadeko and Abraham Femi Afolayan*, "A CRITICAL APPRAISAL OF THE CYBERCRIMES ACT, 2015 IN NIGERIA" Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada, July 24 -28, 2016.

33 "The Legal Framework for Cyber Crimes in Nigeria" https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 9th September 2025.

34 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 22. See also:"10 Things to know about Nigeria's Cybercrime Act 2015" https://lawpadi.com/10-things-to-know-about-nigerias-cybercrime-act-2015/ accessed on 9th September 2025.

35 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 24.

discourse.[36] The amended definition under Section 58 describes cyberstalking as "a course of conduct, directed at a specific person that would cause a reasonable person to feel fear." This legal development reflects ongoing tensions between regulating cyber offenses and protecting freedom of expression in Nigeria.

vi. Cybersquatting: Cybersquatting is a crime under Nigerian law as defined in Section 25 of the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015. It involves the intentional registration or use of a domain name that is identical, similar, or confusingly similar to a trademark, business name, personal name, or other registered name belonging to an individual, corporate body, or government entity in Nigeria, without authorization or right. The purpose of cybersquatting is to interfere with the rightful use of the domain name by its owner, often to profit, mislead, destroy reputations, or prevent the legitimate registration or use. The offense is punishable by imprisonment for up to 2 years, a fine of up to 5 million Naira, or both. Courts can order cyber-squatters to relinquish the disputed domain or name to the lawful owner. The Act does not explicitly provide civil remedies for financial damages but empowers criminal prosecution and court orders for forfeiture.[37]

vii. Phishing and malware: The Act criminalizes sending fraudulent electronic messages and deliberately spreading viruses or malware that damage or disrupt computer systems, networks or data through fraudulent electronic communications or malicious code dissemination.[38] Phishing is defined as the fraudulent means of acquiring sensitive information such as usernames, passwords, or credit card details via electronic communication like emails or instant messages. Penalties include a term of imprisonment of at least three years or a fine of at least 1 million Naira, or both upon conviction, and if such offenses result in substantial loss or damage, penalties increase to a minimum of five years imprisonment or a fine of at least 10 million Naira, or both.

The Cybercrime Act empowers relevant authorities to prosecute these offenses to protect information integrity, cybersecurity, personal data privacy, and prevent financial theft or damage.[39] Restitution orders may be enforced to compensate victims of phishing or malware attacks.[40]

36 "SERAP takes Tinubu govt, governors to ECOWAS Court over 'misuse of Cybercrimes Act" https://serap-nigeria.org/2025/01/12/serap-takes-tinubu-govt-governors-to-ecowas-court-over-misuse-of-cybercrimes-act/ accessed on 9th September 2025.

37 "Cybersquatting in Nigeria: What is Cybersquatting in Nigeria" https://lawpadi.com/cybersquatting-in-nigeria/ accessed on 9th September 2025.

38 The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and Cybercrimes (Prevention, Prohibition, Etc.) (Amendment) Act 2024, Section 32.

39 *Michael Akerele and Anastasia Edward*, "Prohibition and Prevention of Phishing in Nigeria" https://lawkernel.ng/prohibition-and-prevention-of-phishing-in-nigeria/ accessed on 9th September 2025.

40 *Ibid*.

II. Constitution of the Federal Republic of Nigeria, 1999 (As Amended)

The Nigerian Constitution primarily guarantees the right to privacy under Section 37, which protects the privacy of individuals' homes, correspondence, telephone conversations, and telegraphic communications. This right is classified as a Fundamental Right, which means it stands above ordinary laws and is essential for civilized existence, as recognized by the Supreme Court.[41]

The landmark Supreme Court case affirming the primacy of Fundamental Rights, including the right to privacy, is *Chief Dr. (Mrs.) Olufunmilayo Ransome-Kuti & Ors. v. The Attorney-General of the Federation*.[42] In this case, the Court held that Fundamental Rights are antecedent to the political society itself and must be zealously protected. The decision emphasized that the right to privacy prohibits unjustified searches and seizures, and any encroachment must be legally justified and procedurally proper.[43]

In the context of searches and seizures, the Constitutional protection implies that law enforcement agencies must obtain a search warrant before entering private premises or accessing private communications. The warrant must specify the area to be searched and the objects to be seized with precision. Failure to comply with these constitutional requirements invalidates any search or seizure, and any evidence obtained as a result may be deemed inadmissible in court.[44]

Therefore, any law enforcement access to personal electronic devices like cell phones or emails during telecom or cybercrime investigations must respect this constitutional mandate. A search and seizure executed without a proper warrant that clearly describes the place and items contravenes Section 37 and the principles outlined in *Ransome Kuti*, rendering such actions unconstitutional and of no legal effect.[45]

Freedom of expression is also guaranteed under Section 39(1) of the 1999 Constitution of the Federal Republic of Nigeria.[46] It encompasses the right to hold opinions, to receive and impart information and ideas, and to communicate without interference. This right is pivotal to a functioning democracy. It ensures that citizens can question their leaders, demand accountability, and participate meaningfully in governance. In *Director of SSS v. Agbakoba,*[47] the Supreme Court affirmed that freedom of expression includes the right to criticize government policy, provided it is done within the law. However, this right is not

41 "Right to Privacy" <https://www.learnnigerianlaw.com/learn/constitutional-law/privacy> accessed on 13th September 2025.

42 *Ransome-Kuti V. AG Fed* (1985) CLR 6(d) (SC). Available at: https://www.hbriefs.com/sc/chief-dr-mrs-olufunmilayo-ransome-kuti-ors-v-the-attorney-general-of-the-federation-ors-1985/ accessed on 13th September 2025.

43 *Ibid*.

44 *Ibid*.

45 *Ibid*.

46 Constitution of the Federal Republic of Nigeria (1999) (as amended), Section 39(1).

47 (1999) 3 NWLR (Pt. 595) 314.

absolute. Section 39(3) and Section 45 of the Constitution provide for certain permissible limitations, which must be reasonably justifiable in a democratic society. Such limitations typically concern national security, public morality, and protection of the rights of others. But any law that seeks to limit a constitutionally guaranteed right must be sufficiently precise. Vague laws are not only inherently unfair but also dangerous, as they create room for abuse by authorities.[48]

Beyond the Constitution, Nigeria is a party to international treaties that reinforce its commitment to free expression. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantees the right to hold opinions without interference and the freedom to seek, receive, and impart information. Likewise, Article 9 of the African Charter on Human and Peoples' Rights, which has been domesticated in Nigeria, recognizes the same freedoms.

III. Economic and Financial Crimes Commission (EFCC) Act, 2004

The Economic and Financial Crimes Commission (EFCC) Act, 2004 establishes the EFCC as Nigeria's principal agency for tackling financial crimes, including those perpetrated through digital means. While the Act does not expressly regulate cybercrime, it grants the Commission broad powers to investigate and prosecute financial fraud, many of which increasingly occur via the internet and telecommunications platforms. This makes the EFCC a frontline enforcer against cyber-enabled financial offenses, notably advance fee fraud popularly known as "Yahoo Yahoo".[49]

Under the Act, the EFCC is empowered to arrest suspects, monitor financial transactions, and prosecute complex financial offenses. These statutory powers extend naturally into the digital sphere, allowing the Commission to target crimes such as internet fraud,

48 The enforcement patterns mirrored these concerns. Notable examples include: Agba Jalingo: Arrested and charged after publishing a story alleging corruption by the Cross River State governor. He was detained for over 100 days without trial. Solomon Akuma: A pharmacist arrested in 2020 over a satirical tweet about the president. He was detained for nearly a year before being arraigned. Joseph Odok: A lawyer arrested for Facebook posts critical of the Cross River State government. These cases highlight how Section 24 was used not just to combat cybercrime, but to suppress dissent and silence criticism. It became increasingly clear that the provision violated the constitutional principle of legality, which demands that offences be clearly defined so that individuals can foresee the consequences of their conduct. See: Ederagobor Prince Dafemike, "Digital Speech on Trial: Section 24 of Nigeria's Cybercrime Act and its Impact on Civil Liberties"; https://download.ssrn.com/2025/6/22/5315568.pdf?response-content-disposition=inline&X-Amz-Security-Token=-Amz-Signature=69071c8cd6578800e754c998d0310b99be4869f8cba39a5a5d5ac78cd5a0bb55&abstractId=5315568 accessed 13th September 2025.

49 *Alokun Ayomide Emmanuel*, "AN ASSESSMENT OF THE ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC) IN COMBACTING CYBERCRIMES IN KWARA STATE, NIGERIA" http://eprints.lmu.edu.ng/5622/1/EDITED%20COPY%20Ayomide%20FINAL%20DISSERTATION.pdf accessed 13th September 2025.

online scams, and identity theft. By leveraging its investigative mandate, the EFCC is able to pursue offenders who exploit cyberspace for illicit financial gain.[50]

In practice, the EFCC works alongside the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended) to build a comprehensive legal regime against cybercrime. Its focus lies in the financial dimension of such offenses, including confiscating illicit proceeds and prosecuting offenders. Thus, the EFCC Act complements Nigeria's cybercrime framework by strengthening institutional capacity to regulate, investigate, and mitigate cyber-enabled economic crimes.

IV. Nigerian Communications Commission (NCC) Act, 2003

The Nigerian Communications Commission (NCC) Act, 2003 regulates telecommunications services and networks across Nigeria, including online communications. Although primarily designed to oversee licensing, service quality, and operations, the Act also supports the fight against cybercrime. Specifically, section 146 empowers the NCC to require licensees, such as telecom service providers to assist in preventing crimes, thereby enabling collaboration with law enforcement in tackling cyber-related offenses.[51]

Furthermore, the Act grants emergency powers under sections 147–149, authorizing the NCC to suspend licenses, control network facilities, or intercept communications during national security threats or public emergencies.[52] These provisions are crucial for protecting critical information infrastructure and ensuring a swift response to cyberattacks. Beyond enforcement, the NCC issues regulations for internet service providers, promotes consumer awareness on cyber risks, and partners with agencies such as the EFCC to counter cyber-enabled fraud.

The NCC's role complements the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended), particularly in relation to lawful interception, data retention, and incident management. Through its Computer Security Incident Response Team (NCC-CSIRT), the Commission coordinates responses to cyber incidents and strengthens national cyber resilience. In this way, the NCC Act not only regulates telecommunications but also plays an integral role in safeguarding Nigeria's cyberspace.[53]

V. Money Laundering (Prohibition) Act, 2022

The Money Laundering (Prevention and Prohibition) Act, 2022 is a Nigerian law that repealed the 2011 Act and established a comprehensive framework to combat money

50 *Ibid*.

51 NCC Act 2003, s 146.

52 Available at: https://www.ppiaf.org/documents/1424 accessed 13th September 2025.

53 Ogugua VC Ikpeze, "Appraising The Institutional Frameworks For Protection Of Rights To Privacy In Nigeria Vis-À-Vis Unauthorized Wiretapping Of Telephone Communications" *UNIZIK LAW JOURNAL* 19, (3) 2023.

laundering and related offenses in Nigeria. Key features include addressing virtual assets, expanding the scope of covered institutions and activities, increasing penalties, and creating the Special Control Unit Against Money Laundering (SCUML) under the Economic and Financial Crimes Commission (EFCC) to strengthen compliance and prevention efforts.[54]

This Act makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of a crime, or an illegal act. All financial institutions are required to report transactions made that are above specified thresholds for individuals and corporate bodies.[55] The threshold is billed at US$10,000 or its equivalent and shall be reported to the Central Bank of Nigeria, Securities and Exchange Commission in writing within 7 days from the date of transaction. The Act is essentially structured to enable the authorities to monitor cash transactions in a bid to tackle money laundering.[56]

VI. Advanced Fee Fraud and Other Related Offences Act

This Act outlaws every form of fraud including obtaining property by false pretence and obtaining funds through unlawful activities.[57] This law obliges industry players including Internet Service Providers and cybercafé operators to register with the EFCC, monitor the activities of internet users, and report any suspicious activities to the EFCC. In the *Federal Republic of Nigeria v. Abdul*,[58] the accused was arraigned on a two-count charge of being in possession of documents containing false pretences contrary to Section 6(8)(b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act. The accused was arrested in a cybercafé in Benin City by a group of EFCC operatives, following a petition to the Commission by a citizen alleging the incidence of Internet crimes *"yahoo yahoo*" activities at the cybercafé.

VII. Nigeria Deposit Insurance Corporation (NDIC) Act

The Nigeria Deposit Insurance Corporation (NDIC) Act is a cornerstone of Nigeria's financial safety framework. It establishes the NDIC as a statutory body tasked with protecting depositors, maintaining confidence in the financial system, and supporting the Central Bank of Nigeria (CBN) in supervising and stabilizing banks. Enacted in 1988 and replaced by the

54 "OVERVIEW OF ANTI-MONEY LAUNDERING LAWS AND COMPLIANCE FOR NIGERIAN BUSINESSES" https://www.resolutionlawng.com/overview-of-anti-money-laundering-laws-and-compliance-for-nigerian-businesses/ accessed 14th September 2025.

55 *Wigwe* (n. 33).

56 *Ibid*.

57 *MuÁzu Saulawa*, "An Overview of the Legal framework of Advanced Fee Fraud and Cybercrime in Nigeria" (2016) 1 (2) *Hasanuddin Law Review*; 195.

58 *FRN vs Abdul-Salam Abubakar* https://corruptioncases.ng/cases/frn-vs-abdul-salam-abubakar accessed 14th September 2025.

NDIC Act 2006,[59] the law provides the legal basis for deposit insurance, bank regulation, and failure resolution.

Under the Act, all licensed banks and financial institutions are required to insure their deposit liabilities with the NDIC. The scheme guarantees payments to depositors up to a maximum limit of ₦500,000 for deposit money banks and ₦200,000 for microfinance banks and mortgage institutions. This ensures that depositors recover part of their funds if a bank fails, which in turn builds public trust in the financial system.

The NDIC also plays a supervisory role, working with the CBN to monitor banks through examinations and surveillance. Where financial distress is detected, the Corporation can intervene by offering financial assistance, taking over management, facilitating mergers or purchase-and-assumption transactions, or liquidating insolvent banks. In liquidation, NDIC is responsible for paying insured deposits promptly and distributing recovered assets fairly.

The Act further imposes obligations and penalties on banks that fail to insure deposits, conceal information, or mismanage depositor funds. NDIC staff are shielded from liability for actions taken in good faith, while the Corporation benefits from tax exemptions. These provisions strengthen enforcement and accountability across the financial sector.

While the NDIC Act is not a cybercrime law in itself, it contributes indirectly to combating cyber-related financial crimes. By requiring banks to insure deposits, report accurate information, and submit to NDIC supervision, the law enforces transparency and accountability, which are critical in detecting and preventing fraud or cyber-enabled theft in banks. NDIC's supervisory powers allow it to monitor financial institutions for irregularities, including suspicious electronic transactions, thereby complementing other cybercrime legislation such as the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. In practice, the NDIC's role helps safeguard depositor funds against both traditional insolvency and modern digital threats.

VIII. Nigeria Data Protection Act (NDPA), 2023

The Nigeria Data Protection Act (NDPA), 2023 is the country's first comprehensive legislation on data privacy and cyber-security. It establishes the Nigeria Data Protection Commission (NDPC) and provides a framework for regulating how personal data is collected, processed, stored, and transferred. The law aligns with international standards such as the EU's GDPR, reflecting Nigeria's commitment to digital trust and security.

Under the Act, organizations must process personal data lawfully, ensure transparency, and respect the rights of individuals to access, correct, erase, or restrict the use of their information. Data controllers and processors are also mandated to adopt technical and organizational measures that safeguard data from breaches, while cross-border transfers are

59 Cap N102 LFN 2010.

only permitted under strict conditions.[60] The NDPC is empowered to enforce compliance, impose fines, and prosecute violations, making the Act a strong tool against data misuse.

In relation to cybercrime, the NDPA strengthens Nigeria's defenses by mandating better data security practices and minimizing risks of identity theft, fraud, and unauthorized access. This is particularly relevant for financial institutions, where customer information is a prime target for cybercriminals. By ensuring responsible handling of sensitive data, the Act reduces opportunities for cyber-attacks and enhances public confidence in digital platforms.[61]

When viewed alongside the NDIC Act (2006), both laws complement each other. The NDIC Act focuses on protecting depositors and ensuring stability within the banking sector by insuring deposits, supervising financial institutions, and managing failed banks. The NDPA, on the other hand, secures personal and financial information, compelling institutions to strengthen cyber-security and privacy measures. Together, they safeguard two critical assets in the modern economy: money and data. In practice, while the NDIC Act helps protect depositors' funds from loss due to insolvency or fraud, the NDPA ensures that individuals' personal data is not exploited by cybercriminals. Both Acts therefore reinforce Nigeria's broader legal framework against cybercrime, complementing the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 to create a more resilient financial and digital ecosystem.[62]

IX. National Information Technology Development Agency Act 2007

The National Information Technology Development Agency Act 2007 created the National Information Technology Development Agency (NITDA) as a regulatory agency for information technology development in Nigeria. It offers guidelines facilitating the establishment and maintenance of appropriate infrastructure for information technology and systems that will enhance national security. It formulated policy for the development and implementation of regulatory framework for information technology to protect internet users as well as the victims.[63]

60 *Patrick Chukwunonso Aloamaka*, "A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms" (2023) *University of Cape Coast Law Journal*; <https://journal.ucc.edu.gh/index.php/ucclj/article/view/1724 accessed 14 September 2025.

61 KPMG, "*The Nigeria Data Protection Act, 2023"* (KPMG Insights, 19 September 2023); <https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023.html_> accessed 14 September 2025.

62 Banwo & Ighodalo, "*Nigeria Data Protection Act: What Individuals, Businesses And Organizations Should Know"* (Grey Matter Concept, 2023) <https://www.banwo-ighodalo.com/grey-matter/nigeria-data-protection-act-what-individuals-businesses-and-organizations-should-know/> accessed 14 September 2025.

63 *Olusola Joshua Olujobi*, "Analysis of the Legal Frameworks for combating Cybercrimes: A Tool for Economic Development in Nigeria" (2021) 2(1*) KWASU LAW JOURNAL*; 1–27.

E. Gaps and challenges

Despite notable progress, the Nigerian legal framework on cybercrime faces several challenges that limit its effectiveness.

I. Enforcement Difficulties and Institutional Capacity

Law enforcement agencies face significant constraints in enforcing cybercrime laws.[64] First, there is insufficient funding, limiting access to modern forensic tools and surveillance technologies needed to track and apprehend offenders. Second, lack of specialized training hampers effective investigation: many officers remain unfamiliar with handling digital evidence or tracing sophisticated attacks. Third, weak inter-agency coordination leads to inconsistent implementation, with overlaps between institutions such as the EFCC, the Nigeria Police Force Cybercrime Unit, and the Office of the National Security Adviser (ONSA).[65]

II. Evolving Technological Threats and Jurisdictional Complexities

Cybercrime evolves faster than legislation. New threats such as crypto-currency fraud, AI-driven scams, deep-fake technology, and ransomware expose gaps in the Cybercrimes Act 2015. These tools enhance the anonymity of perpetrators, complicating the attribution process.[66] Encryption and virtual private networks (VPNs) further shield criminals, making identification and prosecution extremely difficult.

The threat landscape has evolved rapidly: INTERPOL and independent analysts report rising use of AI (deep-fakes, voice-cloning), crypto-enabled fraud and large-scale social-engineering campaigns; these fast-moving techniques often outpace existing statutes and enforcement playbooks, creating legislative and operational gaps.[67]

In addition, cybercrime is inherently transnational. Nigerian cybercriminals often operate across borders, targeting victims in multiple jurisdictions. This raises complex questions of jurisdiction and applicable law. Although Nigeria is a signatory to some international

64 *Ukasha Ismail*, "The Nigeria Police Force and Cybercrime Policing: An Appraisal" (Dutse Journal of Criminology & Security Studies 2022); https://www.researchgate.net/publication/362395951_The_Nigeria_Police_Force_and_Cybercrime_Policing_An_Appraisal accessed 14 September 2025.

65 *E. Ajayi*, "Challenges to Enforcement of Cybercrimes Laws and Policy in Nigeria" (2016) 2(1) *Journal of Internet and Information Systems* https://academicjournals.org/journal/JIIS/article-full-text-pdf/37DAF9858183 accessed 14 September 2025.

66 *Ibid.*

67 INTERPOL, *Africa Cyberthreat Assessment Report 2025* (INTERPOL, 2025) <https://www.interpol.int/content/download/23222/file/2025%20Africa%20Cyberthreat%20Assessment%20Report.pdf> accessed 14 September 2025.

instruments, limited cooperation with foreign agencies and conflicting legal systems hinder timely investigations.[68]

III. Inadequate risk management practices

Many organizations in Nigeria lack comprehensive risk management strategies for cybersecurity. Thus, insufficient investment in security infrastructure, lack of regular updates, and poor incident response plans can leave systems vulnerable to attacks and data breaches.

IV. Insufficient legal framework and enforcement

While Nigeria has established various legal frameworks to combat cybercrime, enforcement can be inconsistent due to resource constraints, lack of specialized personnel, and bureaucratic challenges. This can hinder the effective prosecution of cybercriminals and deter the implementation of robust preventive measures.

V. Governance, Human Rights, and Public Awareness Issues

Another challenge is the potential misuse of cybercrime laws. For example, the cyberstalking provisions under Section 24 of the Cybercrimes Act though amended following judicial pronouncements are criticised for vague wording that could be weaponised to stifle dissent, restrict press freedom, or criminalise legitimate online expression.[69] Low digital-security awareness among many users (phishing, romance/crypto scams, and SIM-swap vectors) increases victimisation. Studies and surveys indicate that public knowledge about cyber risks and reporting channels is limited; awareness campaigns and consumer-protection measures are repeatedly recommended to reduce the pool of vulnerable victims.[70]

VI. Data Privacy Concerns

There are also data privacy concerns. The tension between state surveillance powers (necessary for tracking cybercriminals) and citizens' rights under the Nigeria Data Protection Act 2023 reflects the delicate balance between security and privacy. Without strong oversight, surveillance can easily slip into human rights abuse.

68 United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (United Nations, Vienna 2021) https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf accessed 14 September 2025.

69 A. Adewopo, "Freedom of Expression and the Cybercrimes Act in Nigeria: A Critical Appraisal" (2020) *Nigerian Law Journal* 23(2).

70 Timothy Ilegbusi, *Cybercrime Prosecution in Nigeria: Challenges & Prospects* (LL.B long essay, University of Ibadan, Feb 2025); <https://www.researchgate.net/publication/390941849_CYBERCRIME_PROSECUTION_IN_NIGERIA_CHALLENGES_PROSPECTS> accessed 14 September 2025.

VII. Potential for misuse (free speech, over-criminalisation)

Observers, diplomatic missions and press-freedom groups have warned that broad or vaguely worded provisions in Nigeria's cyber laws have sometimes been applied in ways that chill journalism and dissent. Recent high-profile detentions and critical commentaries demonstrate the risk that anti-cybercrime rules can be misapplied to suppress legitimate speech.[71]

VIII. Lack of specialised courts & judicial expertise

Technically complex evidence (logs, metadata, block-chain tracing, deep-fake analysis) needs judges and prosecutors with digital evidence skills; the absence of dedicated cybercrime or specialised technology courts means ordinary criminal dockets handle these matters causing delays, evidentiary mistakes, and inconsistent rulings. Policy reviews recommend specialized judicial tracks or training schemes.[72]

F. Recommendations for Strengthening the Regulation of Cybercrime in Nigeria

Addressing enforcement difficulties requires Nigeria to prioritize capacity building among its law enforcement agencies. The creation of accredited regional forensic laboratories, adequately funded and staffed, would provide investigators with access to modern tools for handling digital evidence. In addition, the establishment of a national certification programme for investigators, prosecutors, and judges would ensure that only those with the requisite technical expertise handle cybercrime cases. Formalised inter-agency coordination, possibly through a National Cybercrime Coordination Centre, would also enhance synergy between institutions such as the EFCC, the Nigeria Police Force, and the Office of the National Security Adviser. These measures, coupled with targeted funding streams from both government and private sector partnerships, would help overcome long-standing institutional and resource deficiencies.

To confront evolving technological threats, Nigerian legislators and regulators must adopt a technology-neutral approach to law-making. Rather than attempting to ban each new tool or platform, the law should focus on harmful conduct and its effects, whether it arises from artificial intelligence, crypto-currency, or other emerging technologies. A standing technical review committee could provide periodic recommendations for statutory updates, ensuring that legislation remains responsive to fast-moving innovations such as deep-fakes and AI-driven scams. At the operational level, strengthening the capacity of the

71 U.S. Embassy & Consulate in Nigeria, "Preventing Misuse of the Cybercrimes Act: Protecting Free Speech And Unlocking Economic Growth (op-ed / statement, 2025)" https://ng.usembassy.gov/preventing-misuse-of-the-cybercrimes-act-protecting-free-speech-and-unlocking-economic-growth/ accessed 14 September 2025.

72 Chaman Law Firm, "9 Cyber Crime Prosecution Breakthrough Challenges In Nigeria" https://chamanlawfirm.com/9-cyber-crime-prosecution-breakthrough-ch/ accessed 14 September 2025.

National Computer Emergency Response Team (CERT) and equipping law enforcement with block-chain and crypto-forensics tools will be vital in improving attribution. Moreover, because cybercrime is inherently transnational, Nigeria should deepen its cooperation with international partners by adopting model mutual legal assistance treaties and signing bilateral agreements that permit expedited transfer of digital evidence.

The development of sound risk management practices within organizations is also essential. Many Nigerian institutions, particularly outside the financial sector, remain vulnerable because of poor cybersecurity infrastructure and weak incident response plans. Regulators should mandate baseline security standards in critical sectors such as banking and telecommunications, requiring organisations to adopt encryption, multi-factor authentication, and patch management protocols. Incident response planning and reporting obligations, tied to oversight by regulators like the NDPC and the CBN, would strengthen institutional resilience. In parallel, the promotion of cyber insurance and incentives for small and medium enterprises to adopt affordable security tools would help spread a culture of risk management across the economy.

Nigeria's legal framework for cybercrime, though relatively robust, still requires refinement. A comprehensive audit of existing statutes is needed to identify overlaps and gaps between the Cybercrimes Act, the Nigeria Data Protection Act, and sectoral regulations. Targeted amendments should clarify key definitions, especially those surrounding unauthorised access, cyberstalking, and electronic evidence. Prosecutorial units with specialised expertise should be established under the Attorney-General's office to assist state agencies and provide uniform standards for electronic evidence admissibility. These reforms would not only enhance consistency in prosecution but also improve conviction rates while safeguarding against misuse.

Governance and human rights concerns must also be addressed. Clear prosecutorial guidelines should be issued to prevent the misuse of cybercrime provisions against journalists, political opponents, or online activists. Judicial and parliamentary oversight mechanisms should review enforcement actions regularly to ensure compliance with constitutional guarantees of free expression. Alongside this, a broad-based public awareness campaign is necessary to improve digital literacy and reduce citizens' vulnerability to phishing, SIM-swap fraud, and online scams. Integrating cyber safety education into school curricula and public service training would further institutionalise awareness. Civil society organisations, too, should be empowered to provide legal support to victims of cybercrime and those wrongfully prosecuted under cyber laws.

The regulation of surveillance and data privacy demands a careful balancing act. Clear procedural guidelines must be developed for law enforcement agencies to request access to personal data in line with the Nigeria Data Protection Act 2023. Judicial authorisation, strict proportionality tests, and audit trails should be mandatory safeguards against abuse. The NDPC should play a central role in oversight by reviewing compliance and auditing agency access to personal data. Embedding such accountability mechanisms will help reconcile the tension between national security imperatives and citizens' fundamental rights.

Concerns about over-criminalisation and vague statutory wording should be resolved through legislative clarification. Offence definitions need to be narrowed, with explicit intent requirements included to avoid criminalising innocent behaviour or legitimate expression. Prosecutors and judges should be trained in the application of digital rights and freedom of expression principles, ensuring that the law protects against harmful online conduct without undermining democracy. Independent review mechanisms or ombudsman institutions could also be created to assess complaints of misuse of cybercrime laws and provide redress where appropriate.

Finally, Nigeria's judiciary must adapt to the technical demands of cybercrime litigation. The establishment of specialised technology courts, or at least designated judges with additional training in digital evidence, would significantly improve the quality and speed of adjudication. Bench books and evidentiary protocols should be developed to guide courts on handling electronic evidence, while a national roster of independent technical experts should be made available to assist in complex cases. These measures would not only reduce delays but also increase confidence in the judiciary's ability to deliver justice in highly technical matters.

G. Conclusion

Nigeria's legal framework on cybercrime has evolved significantly with the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and its subsequent amendment in 2024. These legislative interventions represent a conscious effort by the Nigerian state to respond to the growing complexity and sophistication of cyber-enabled crimes within an increasingly digital society. In theory, the framework is largely comprehensive, as it criminalises a wide spectrum of cyber-related offences, establishes regulatory and institutional mechanisms for enforcement, and aligns, to some extent, with international best practices in the fight against cybercrime.

Notwithstanding these commendable strides, the effectiveness of Nigeria's cybercrime regime remains significantly constrained by persistent implementation challenges. Chief among these are inadequate technical expertise and infrastructural capacity within law enforcement and prosecutorial agencies, limited public awareness of cybercrime laws and digital safety obligations, weak inter-agency coordination, and insufficient international cooperation, which is an essential component given the transnational nature of most cyber offences. Furthermore, the rapid pace of technological innovation continues to outstrip legislative and institutional responses, thereby exposing gaps in the law and complicating enforcement efforts.

In light of these challenges, it is evident that the mere existence of a robust statutory framework is insufficient to effectively combat cybercrime. There is an urgent need for sustained capacity building for relevant institutions, continuous legislative review to keep pace with emerging technologies, enhanced public sensitisation, and stronger collaboration with international partners. Addressing these issues is critical not only to improving the

enforcement of cybercrime laws but also to strengthening Nigeria's overall digital security architecture. Ultimately, a functional and adaptive cybercrime framework will contribute significantly to national security, economic stability, public confidence in digital platforms, and Nigeria's integration into the global digital economy.