SOCIAL MEDIA FACILITATED CYBERCRIMES IN NIGERIA AND THE CHALLENGES OF LEGAL ENFORCEMENT*

Abstract
The proliferation of social media platforms in Nigeria has transformed communication, networking, and business. However, alongside these benefits is the exploitation of these platforms by cybercriminals for fraudulent activities, identity theft, phishing, and other cybercrimes. This paper critically examines the role of social media in facilitating cybercrime in Nigeria, investigating the platforms used, common methods of cyberattacks, socio-economic motivations, and the limitations of legal and institutional frameworks. It also evaluates responses from law enforcement agencies and the efficacy of existing cybersecurity legislation. Using a doctrinal approach, the study advocates for a multi-stakeholder response involving regulatory reforms, digital literacy, and transnational cooperation. It recommends for the strengthening of the existing legislative and regulatory frameworks through review of the Cybercrimes Act, 2015; constant education and enlightenment of the populace on the dangers of negative use of social media; inter-agency co-operation in the fight against crimes committed using the social media, among others.

Keywords: Social media, cybercrime, Nigeria, digital fraud, cyber legislation, online security

1. Introduction

The 21st century has seen a dramatic evolution in communication technologies, particularly through social media, which has transformed interactions, business, and information access globally.[1] In Nigeria, the rise of social media is fueled by widespread smartphone use and affordable internet, making it one of the leading African nations in active social media usage, with platforms like Facebook, WhatsApp, Instagram, and TikTok being popular.[2] However, this growth has a darker side: the surge in cybercrime. Criminals exploit the anonymity and openness of these platforms for various illegal activities, such as fraud, phishing, and identity theft.[3] Nigeria's socio-economic challenges, like poverty and unemployment, coupled with weak regulatory frameworks, exacerbate this vulnerability.[4] The phenomenon of 'Yahoo Boys',[5] who impersonate affluent individuals online to defraud victims, illustrates the problem. This not only harms Nigeria's international reputation but also erodes trust in digital systems, resulting in significant economic losses.[6] While the Cybercrimes Act of 2015 is a step forward, enforcement remains inconsistent, and many crimes go unreported due to victims' lack of digital literacy and law enforcement limitations.[7] The paper uses a socio-legal framework to analyze the relationship between social media and cybercrime in Nigeria, exploring contributing factors and legal responses. It advocates for coordinated strategies, including regulatory reforms, digital literacy initiatives, and enhanced law enforcement and international collaboration, to tackle cybercrime effectively.

2. Conceptual Clarification

Cybercrime

Cybercrime includes various illegal activities conducted via computer systems and the internet, such as online fraud, hacking, malware distribution, cyberterrorism, etc.[8] Its definitions and prevention strategies are complicated by the internet's borderless nature. The UNODC categorizes cybercrime into two main types: crimes targeting computer devices and those that use computers to facilitate traditional crimes. As reliance on digital infrastructure increases, especially in developing countries like Nigeria, cybercrime is on the rise, exacerbated by low digital literacy and cybersecurity awareness. Legal scholars highlight the evolving nature of cybercrime, which differs from conventional crime in scale, speed, and invisibility. This evolution poses challenges for investigators and legal systems, particularly in countries with outdated laws. In Nigeria, cybercrime, often termed 'Yahoo Yahoo,' typically involves online scams. The National Assembly passed the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015, amended in 2024, to address these issues. However, critics point to inadequate implementation and the lack of resources for enforcement agencies to handle complex digital evidence especially in view

***By Matthew E. NWOCHA, LLB, BL, LLM, PhD,** Professor of Jurisprudence and International Law, Ebonyi State University, Abakaliki, Tel: 07035909335;
***Chioma Vivian ITESHI, LLB, BL, LLM, PhD,** Senior Lecturer, Faculty of Law, Ebonyi State University, Abakaliki**,** Tel: 08035076023; and
***Paul Mgbada AWADA, LLB, BL, LLM, PhD (in view),** Faculty of Law, Ebonyi State University, Abakaliki, Email: pmawada@gmail.com; Tel: 08038767017; 08087596338

[1] M. Sheikh, 'Rise of Social Media and its Impact on Global Communication' (27 November 2023) <https://dailytimes.com.pk/1148420/rise-of-social-media-and-its-impact-on-global-communication/> accessed 30 March 2025.
[2] Nigerian Communications Commission (NCC), *National Cybersecurity Policy and Strategy* (NCC, 2021) 7.
[3] O. Damilola, A. Emmanuel and P. Bich Ngoc, 'Cybercrime on Social Media in Nigeria: Trends, Scams, Vulnerabilities and Prevention' Proceedings of the Cyber Secure Nigeria Conference, Nigerian Army Resource Centre (NARC), Abuja, Nigeria, 11–12 July 2023, 143–150.
[4] O. Olayemi, 'A Socio-legal Analysis of Cybercrime in Nigeria' [2014] *Journal of Internet Law (*16) 174.
[5] These are internet fraudsters who use social engineering techniques to deceive victims.
[6] C. Ojedokun and C. Eraye, 'Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria' [2012] *International Journal of Cyber Criminology* (7) 564.
[7] U. Onuora, *Law and Cybercrime in Nigeria: A Critical Appraisal* (Donovon Press, 2018) 144; A. Ayoade, 'Cross-Border Challenges in the Enforcement of Cyber Laws in Nigeria' [2020] *Nigerian Journal of Law and Technology* (18) 67.
[8] B. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger, 2010) 5.

of its cross-border nature.[9] In summary, cybercrime presents significant risks to national security, economic development, and personal privacy, complicated by the global nature of the internet and the lag in legal reforms.

Social Media

Social media comprises web-based platforms that facilitate interactive dialogue through user-generated content, including popular sites like Facebook, X[10], Instagram, and TikTok. Defined by Kaplan and Haenlein as Internet-based applications rooted in Web 2.0, social media emphasizes user participation in content creation. Boyd and Ellison classify these platforms as networked communication systems that enable users to create profiles and connect with others, distinguishing them from earlier online formats. In Nigeria, social media's rapid growth is driven by improved mobile internet access and a youthful population, with over 100 million Nigerians engaging daily for personal interaction, political activism, and entrepreneurship. However, the anonymity and real-time sharing features of these platforms have led to increased cybercrime, including identity theft and social engineering. The unregulated nature of social media raises concerns about governance and ethical usage, as it can facilitate misinformation, trolling, and other harmful behaviors. While social media fosters engagement and empowerment, it also poses risks to cybersecurity and national development.[11] Addressing the intersection of social media and cybercrime requires a multi-faceted approach, including digital literacy, platform regulation, international cooperation, and effective legal enforcement.

3. Typologies of Social Media-Facilitated Cybercrime in Nigeria

Internet Fraud (Yahoo Yahoo)

In Nigeria, a significant form of cybercrime linked to social media is internet fraud, commonly known as 'Yahoo Yahoo.' This term originated from early email scams using Yahoo Mail and has evolved to include various fraudulent activities on platforms like Facebook, Instagram, WhatsApp, TikTok, and X.[12] Fraudsters, often referred to as 'Yahoo Boys,' utilize social engineering techniques to exploit emotional vulnerabilities, particularly through romance scams that trick victims into sending money under false pretenses.[13] The socio-economic landscape of Nigeria, characterized by high youth unemployment, poverty, and societal admiration for wealth, contributes to the rise of Yahoo Yahoo as a perceived legitimate path to success. Social media not only facilitates these crimes but also normalizes and celebrates fraudulent lifestyles, further perpetuating the cycle of cybercrime.[14] Additionally, some individuals engage in 'Yahoo Plus,' a variant that includes ritualistic elements, complicating detection and enforcement.[15] The situation has now been made worse by the incursion of the Artificial Intelligence (AI)[16] genre. Although the Nigerian Cybercrimes Act of 2015 provides a legal framework to combat these activities, enforcement is hindered by technological and institutional challenges. Overall, Yahoo Yahoo is a deeply rooted issue within Nigerian society, exacerbated by the influence of social media.[17]

Phishing via Social Media Platforms

Cybercriminals often create fake social media profiles that impersonate financial institutions, government agencies, or acquaintances to initiate contact with victims. They use direct messages or links in posts to direct users to counterfeit websites, where sensitive information like login credentials and banking details is collected.[18] Phishing may also be disguised as investment opportunities or scholarship offers, leveraging social engineering tactics that exploit urgency, fear, or curiosity. This method is particularly effective on social media, where users' trust in familiar interfaces makes it more dangerous than traditional phishing emails.[19] In Nigeria, this approach has led to widespread fraud, especially during economic crises or elections, prompting users to act quickly without verifying information. For instance, fake customer service accounts may contact users seeking help, only to request sensitive data like OTPs[20] or BVNs[21]. Despite efforts in digital literacy and platform detection systems, phishing remains a significant threat due to its low cost, broad reach, and ability to adapt to new social media features.

Identity Theft and Impersonation

Identity theft on social media involves the unauthorized use of another person's identity—name, photos, or other personal information—to deceive others, often for fraudulent or malicious purposes. In Nigeria, this crime has risen significantly,

[9] Ss. 6, 8, 9, 11, 12, 14 & 16 of the Act; U. Onuora (n 7) 144.
[10] Formerly 'Twitter'
[11] Olayemi (n 4) 174; Ayoade (n 7) 67.
[12] O. Ayandele and O. Popoola, *'Yahoo Yahoo: Cyber-enabled Crime and Criminality in Nigeria'* (2019) <https://doi.org/10.2139/ssrn.3999317> accessed 29 March 2025.
[13] C. Ojedokun and C. Eraye (n 6) 565; A. Chukwudi, 'Romance Scams and the Internet: A Study of Online Deception in Nigeria' [2021] *African Journal of Criminal Justice* (13) 223.
[14] M. Ibrahim, *Cybercrime and Youth Subcultures in West Africa* (Justice Watch Press, 2021) 158.
[15] E. Alemika, 'The Ritualisation of Cybercrime in Nigeria: A Study of 'Yahoo Plus'' [2022] *Nigerian Journal of Criminology and Security Studies* (18) 203.
[16] Development of computer systems that can perform tasks that traditionally require human intelligence.
[17] A. Ajayi, 'Yahoo Yahoo and the Digital Subculture of Nigerian Youths' [2020] *Journal of Cyber Studies in Africa* (6) 97.
[18] O. Arowosegbe, *Cybercrime in the Digital Age: Legal and Social Responses in Nigeria* (Equity Press, 2021) 113.
[19] A. Adebayo and A. Adepoju,' 'Social Media Phishing and Its Implications for Financial Crime in Nigeria' [2020] *African Journal of Criminology and Forensic Studies (*12*)* 241.
[20] One-time passwords
[21] Bank Verification Numbers

aided by the ease with which personal data can be harvested from public profiles.[22] Perpetrators typically clone the social media accounts of real individuals and then contact their followers to solicit money under false pretenses. This practice, also known as impersonation fraud, has become rampant on platforms like Facebook and Instagram, where trust among contacts is exploited to facilitate scams.[23] In more sophisticated cases, stolen identities are used to apply for loans, access private accounts, or blackmail victims. This typology of cybercrime is particularly problematic because victims are often unaware that their identity has been stolen until financial or reputational damage has occurred. Moreover, the virality and shareability of content on social media accelerate the reach and impact of these crimes, making containment difficult.[24] Weak cyber hygiene and lack of user awareness deepen vulnerability to impersonation crimes.[25] Identity theft is also used in a politically charged environments to create fake profiles to spread misinformation, discredit opponents, or incite unrest.

Fake Business Accounts and E-Commerce Scams

The typology describes the creation of fake profiles on platforms like Instagram, Facebook Marketplace, and WhatsApp Business to impersonate legitimate businesses. Cybercriminals exploit the informal trust-based nature of social commerce in Nigeria,[26] targeting young consumers and small-scale entrepreneurs who use these platforms for transactions. The lack of regulatory oversight, transaction insurance, and weak consumer protection laws facilitate this fraud. Perpetrators can easily evade capture by frequently changing their identities, making it difficult to hold them accountable.

Money Doubling and 'Investment' Scams

The money doubling scam in Nigeria has evolved from traditional '419'[27] frauds into elaborate investment schemes on social media, exploiting economic hardship and social desperation. Scammers create fake fintech accounts or impersonate religious figures, promising unrealistic returns on small investments. They bolster their claims with fabricated testimonials and staged videos shared virally.[28] A notable variant is the 'Giver's Circle' or 'Loom,' a pyramid scheme that collapsed in 2019 but has spawned similar scams. The use of celebrity influencers lends these schemes credibility, making victims reluctant to report due to shame or threats.[29] Efforts by the Nigerian government, including cyber surveillance and consumer alerts, face challenges due to the decentralized nature of social media.

Cyberbullying and Blackmail on Social Media

Cyberbullying and blackmail are serious forms of cybercrime in Nigeria, using threats, humiliation, and false accusations to inflict emotional and psychological harm via social media platforms. Unlike scams aimed at financial gain, these crimes exploit personal vulnerabilities, leading to trauma and social isolation, particularly among teenagers and women who are heavily engaged online.[30] Blackmail, often termed sextortion, involves the use of intimate images or personal information for extortion, with WhatsApp and Snapchat being common platforms due to their encryption features that hinder detection.[31] A troubling trend is the non-consensual sharing of explicit materials, known as 'revenge porn,' affecting individuals across various demographics, including minors and celebrities. The pervasive shaming culture on Nigerian social media exacerbates the impact of these crimes, making victims reluctant to report incidents due to fear of exposure and societal stigma.[32] Legal recourse is often hindered by secondary victimization from law enforcement and pressures to settle cases privately, allowing perpetrators to act with little consequence.[33]

Cyberstalking and Surveillance Abuse

Cyberstalking is a serious and often underreported form of cybercrime in Nigeria, characterized by persistent harassment and monitoring through digital means, especially on social media. It primarily affects public figures, ex-partners, journalists, and legal professionals, with common cases involving obsessive admirers or jealous e[34]x-lovers.[35] The anonymity afforded

---

[22] J. O. Olatunde, *Cybercrime and Nigerian Law Enforcement: Challenges and Prospects* (Spectrum Books, 2021) 88.

[23] B. E. Eze, *Cybersecurity and Cybercrime Legislation in Nigeria: An Appraisal* (Grace Publishers, 2021) 284.

[24]T. Kayode-Adedeji and others, 'Social Media and Identity Theft Implications on Nigerian Victims and International Economy' (IGI Global, 2020) 823–836.

[25] S. Ndukwe, 'Digital Identity Theft and the Limits of Cybersecurity Legislation in Nigeria' [2020] *Nigerian Law Review* (8) 152.

[26] A. O. Adewumi**,** *Social Media Fraud and the Nigerian Legal Response* (Temidayo Press, 2020) 117; C. F. Okoro**,** *Cybercrime and Digital Deception in Nigeria* (Justice Watch Press, 2022) 151.

[27] This appellation is derived from s.419 of the Nigerian Criminal Code

[28]O. Salami, 'Financial Illusions in the Digital Space: An Analysis of Internet-Based Ponzi Schemes in Nigeria' [2020] *West African Journal of Cyber Governance* (12) 190.

[29] K. Obialor, 'Social Media Influencers and the Promotion of Cybercrime in Nigeria' [2021] *Journal of Media and Cyber Ethics* (9) 219.

[30]C. U. Okafor, *Cybercrime and Social Media Misuse in Nigeria: Legal and Social Perspectives* (Lexis Communications, 2020) 157; C. Nwokolo, 'Cyberbullying in Nigerian Schools: The Emerging Role of Social Media Platforms' [2021] *West African Journal of Digital Education and Safety* (19) 176.

[31]T. Adeyemi and E. Ude, 'WhatsApp and Sextortion: Hidden Faces of Blackmail in Nigeria's Digital Space' [2022] *Journal of Criminology and Human Rights* (11) 154.

[32]M. Obaro and F. Ekpo, 'Revenge Porn and the Moral Panic of Sexuality on Nigerian Social Media' [2020] *Journal of Media Law and Ethics in Africa* (7) 198.

[33]I. Ibikunle, 'Digital Trauma and Legal Gaps: A Feminist Analysis of Cyberbullying in Nigeria' [2021] *Nigerian Journal of Gender and Cyber Law* (13) 211; A. B. Sogunle, 'Cybercrimes (Prohibition, Prevention, etc.) Act 2015: Challenges to Enforcement' [2021] *Journal of Law and Judicial System* (4) (1) 1-11.

[34]R. Obaje, 'Cyberstalking in Nigeria: Legal Provisions, Enforcement Challenges and Gender Implications' [2022] *Journal of Women, Law and Cyber Justice* (11) 183.

[35] T. K. Adeyemi, *The Evolution of Cybercrime in Nigeria: Trends and Responses* (Cyberlaw Publications, 2022) 203.

by digital platforms, combined with a lack of robust privacy regulations, enables stalkers to track victims' real-time locations and activities.[36] Despite being criminalized under the Cybercrimes Act of 2015, enforcement is weak due to challenges in digital evidence handling, leading many victims—particularly women—to have their complaints dismissed or inadequately addressed.[37]

4. Legal and Institutional Frameworks in Combating Social Media-Facilitated Cybercrime in Nigeria

Nigeria recognizes the growing threat of cybercrime and has established several institutional and legislative measures to combat it. Despite these efforts, challenges like enforcement gaps, jurisdictional limitations, and socio-political issues impede their effectiveness. This section explores the main legal frameworks and institutions involved in addressing cybercrimes related to social media in Nigeria.

4.1 Legal Framework

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

The Constitution of the Federal Republic of Nigeria, 1999 (as amended), emphasizes that the primary purpose of government is to ensure the security and welfare of its citizens.[38] It guarantees the privacy of individuals, including their homes and communications.[39] To uphold these rights, the government has enacted laws and created institutions aimed at protecting citizens' security and privacy, particularly in relation to social media violations.

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

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 remains the principal legislation governing cyber offences in Nigeria. The Act is comprehensive in scope, extending its provisions to cover crimes committed through social media, online platforms, and other forms of Information and Communications Technology (ICT). Notably, it serves as a legal framework that aligns with global efforts to combat cybercrime while also addressing the unique challenges faced by Nigeria in securing cyberspace and protecting citizens from digital harm.[40] Section 24 of the Act addresses cybercrimes, particularly those exacerbated by social media, and aims to mitigate their negative impact on victims' mental health.[41] However, it has faced criticism for its ambiguity, leading to concerns about selective enforcement against political dissenters and potential violations of fundamental rights.[42] Additionally, Section 38 establishes a National Cybersecurity Fund to bolster the government's efforts in combating cybercrime through collaboration. Despite these initiatives, challenges in implementation persist, particularly as international social media platforms often resist compliance with Nigerian regulations due to data privacy and jurisdictional issues. An example of this tension is the seven-month ban on Twitter by the Nigerian government in response to the platform's removal of a government tweet on the civil war[43].

Nigerian Communications Commission (NCC) Act 2003

The Act complements the regulation of Nigeria's telecommunications sector by empowering the Commission, under Section 34 of the NCC Act, to supervise telecom service providers. It ensures their compliance with national security requirements and mandates cooperation with law enforcement on issues related to cybercrime and cybersecurity.[44] he implementation of the NCC Act has been inconsistent, similar to the Cybercrimes Act, primarily due to insufficient resources, inadequate capacity building, and a lack of technical expertise in the regulatory bodies responsible for enforcement.

Evidence Act 2011 (as amended in 2023)

The Evidence Act 2011, amended by the Evidence (Amendment) Act 2023, is crucial in Nigeria's fight against cybercrimes on social media by enhancing the admissibility and authentication of electronic evidence in the prosecution of cyber offences.[45] Section 84 is key, allowing electronically generated evidence in court, provided it comes with a certificate of authenticity from a qualified individual. This requirement helps ensure the integrity of often manipulable digital evidence.[46] The 2023 amendment clarifies ambiguities in Section 84, especially regarding automated systems like cloud platforms, and empowers judges to use discretion in admitting electronic records to prevent injustice, particularly when time-sensitive data is involved. Despite challenges due to a lack of specialized training in digital forensics among judges and lawyers, Nigerian courts are increasingly accepting digital evidence, as seen in the FRN v. Danladi case,[47] where social media messages were validated. The Evidence Act complements the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which criminalizes cyber offenses, by providing

[36]U. Eze and J. Audu, 'Tracking Without Consent: Social Media and Surveillance Abuse in Nigeria' [2020] *Nigerian Journal of Digital Rights and Law (*14) 194.
[37] T. K. Adebanjo, *Legal Responses to Gender-Based Cybercrime in Nigeria* (Temple Gate Publishing, 2022) 211.
[38] Section 14(1)(b) of the Constitution
[39] *Ibid* s.37
[40] Eze (n 27) 284.
[41] I. M. Okon, *Cybercrime and Mental Health: A Nigerian Perspective* (Digital Press Nigeria, 2020) 156.
[42] Adebanjo (n 41) 215.
[43] https://en.wikipedia.org/wiki/Blocking_of_Twitter_in_Nigeria Retrieved on 2/08/2025
[44] Eze (n 27) 289.
[45] A. Okoroafor, 'Admissibility of Digital Evidence in Nigeria: An Appraisal of Section 84 of the Evidence Act 2011' [2021] *Nigerian Journal of Cyber Law and Policy* (12) (2) 45, 48; A. A. Adebayo, *Cybercrime Law and Digital Evidence in Nigeria* (Princeton Publishing, 2022) 113–117.
[46]T. Agomo, 'The 2023 Evidence Act Amendment and the Evolution of Digital Justice in Nigeria' [2023] *Journal of Nigerian Legal Innovations* (5) (1) 101, 103–105.
[47] (2020) LCN/14301(CA); CA/A/687C/2017.

procedural mechanisms for evidence integrity in court aligning same with international standards which reinforces the judiciary's role in cybercrime deterrence.[48]

National Information Technology Development Agency (NITDA) Act
The NITDA Act 2007 empowers the Agency to regulate and promote information technology in Nigeria. Specifically, section 6 authorizes NITDA to develop guidelines for electronic governance and monitor IT usage across sectors. Section 17 enables the Agency to provide advisory and enforcement services on IT regulations. Through these provisions, NITDA asserts legal authority to issue directives that influence cybersecurity practices in both public and private sectors.[49]

4.2 Institutional Framework

Nigeria Police Force (NPF) – Cybercrime Unit
The Nigeria Police Force (NPF) Cybercrime Unit, part of the Force Criminal Investigation Department (FCID), was established under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the Police (Establishment) Act 2020 in response to the increasing complexity of internet-related offences. It aims at providing focused mechanisms for digital forensic investigations in accordance with national policy directives.[50] The Unit has developed digital forensics capabilities and emphasizes data preservation while collaborating with both national and international agencies, including INTERPOL and ngCERT.[51] Court rulings, such as in *FRN v Danladi*[52] and *FRN v Osasuyi & Ors*[53], affirm the Unit's authority in handling digital evidence and prosecuting cybercrime. However, the Cybercrime Unit faces significant challenges, including outdated investigative tools, poor inter-agency coordination[54], inadequate training in new technologies, jurisdictional ambiguities, and slow legal assistance processes. It seeks to enhance its capacity through partnerships with the Nigerian Communications Commission (NCC) and NITDA, highlighting the need for institutional synergy for effective cybercrime enforcement in Nigeria's complex framework.

Economic and Financial Crimes Commission (EFCC)
The Economic and Financial Crimes Commission (EFCC) was established under the EFCC Act 2004 to investigate, prevent, and prosecute financial crimes, including those conducted via social media, such as phishing and online scams.[55] Social media has become a key platform for cybercriminals in Nigeria, facilitating identity theft and fraud. The EFCC's Cybercrime Section has conducted significant sting operations, often collaborating with the Nigeria Police Force and international agencies like the FBI and Interpol.[56] The Cybercrimes Act 2015 mandates the EFCC to enforce various provisions related to cybercrime.[57]

The Commission maintains a public record of prosecuted offenders, including foreigners, highlighting the use of social media in these crimes.[58] In 2021, the EFCC secured 2,220 convictions,[59] and in 2024, it achieved 4,111 convictions,[60] many linked to social media offenses. However, critics argue that the EFCC sometimes prioritizes high-profile arrests over effective cyber governance, suggesting that its approach may criminalize poverty and neglect the underlying socio-economic issues, such as unemployment, that drive youth toward cybercrime.[61]

National Information Technology Development Agency (NITDA)
The Nigeria Data Protection Regulation (NDPR) 2019 is a key tool for the National Information Technology Development Agency (NITDA), focusing on personal data protection against cyber-attacks. It mandates data controllers to implement safeguards and imposes penalties for non-compliance to deter data misuse.[62] In 2022, NITDA introduced cybersecurity guidelines for government ministries, setting minimum standards for network security and incident response to protect sensitive data.[63] NITDA collaborates with stakeholders like the Nigerian Communications Commission and the Nigeria Police Force's Cybercrime Unit, as part of the National Cybersecurity Policy and Strategy (NCPS) 2021,[64] which promotes a coordinated national approach to cybersecurity.

---

[48]N. Egbunike, 'Judicial Approaches to Electronic Evidence in Nigeria: Lessons from Recent Cybercrime Trials' [2023] *Nigerian Law Review* (6) (1) 54, 58.
[49] <https://nitda.gov.ng/> accessed 20 March 2025.
[50] B. Ogbonna, 'Challenges Facing Cybercrime Investigation in Nigeria: A Police Perspective' [2021] *Criminal Justice Policy Review Nigeria* (7) 173; Sections 39,41 and 44 of the Cybercrime Act; Sections 4 and 33(1)(g) of the Police (Establishment) Act
[51]C. Paul and E. V. Victor, 'Digital Divide and Uptake of Public E-Service in Nigeria: A Narrative Review' [2023] *Journal of Technology Innovations and Energy* (2) (4) 27–41.
[52] (2020) LCN/14301(CA); CA/A/687C/2017
[53] (2018) LPELR-43835(CA).
[54] I. K. Ndukwe, '*Law Enforcement and the Digital Divide in Nigeria'* [2023] *Journal of Digital Governance* (3) (2) 85–92, 89.
[55] EFCC Act 2004, s. 6
[56] A.S. Yusuf, 'Cybercrime and the Nigerian Legal Framework: A Critical Appraisal' [2021] *Journal of Digital Law and Policy* (5) (2) 116.
[57] Cybercrimes Act, s.8; O. S. Adekunle, *Cybersecurity Law and Governance in Nigeria* (Spectrum Books Ltd, 2020) 83–85.
[58] Economic and Financial Crimes Commission, *EFCC 2022 Annual Report* (Economic and Financial Crimes Commission, 2023) 41–45.
[59] efcc.gov.ng. Accessed on 6/08/2025
[60] https://punchng.com Accessed on 6/08/2025
[61]T. I. Ogbonnaya and A. Bello, 'Youth, Internet Fraud and the Limits of State Enforcement: Rethinking Nigeria's Cybercrime Strategy' [2022] *African Journal of Criminology and Justice Studies* (16) (1) 25; T. Awe, 'The EFCC and the Politics of Yahoo Boy Raids in Nigeria' [2021] *Journal of Financial Crime Studies* (9) 142
[62] M. C. *Ogwezzy, 'Data Protection in Nigeria: Evaluating the Efficacy of the NDPR' [2020] Babcock University Law Journal* (3) (1) 52–54.
[63] National Information Technology Development Agency (NITDA), *Guidelines for Cybersecurity for MDAs* (NITDA, 2022) 3–5; G. *Ayoade and A. Hassan, 'Cyber Hygiene and Institutional Compliance in Nigeria' [2022] ICT & Law Review (4) 88–90.*
[64] National Cybersecurity Policy and Strategy (NCPS) 2021*, Objectives 3 & 6; O. A. Idowu, 'Towards a Multi-Agency Framework for Combating Cybercrime in Nigeria' [2021] Nigerian Journal of Cyber Law and Policy (2) 121–124.*

Through regulatory frameworks and public awareness efforts, NITDA has strengthened Nigeria's cybersecurity landscape. However, there is an urgent need to update the NITDA Act 2007 to better align with its expanded role in cybercrime prevention and digital security enforcement.[65]

4.3 Some Challenges in the Enforcement of the Legal and Institutional Frameworks in Combating Social Media-Facilitated Cybercrime in Nigeria

Inadequate Inter-Agency Coordination

The lack of effective coordination among agencies addressing cybercrime in Nigeria is a significant challenge. Multiple institutions are involved in enforcing cybercrime laws, but their fragmented approaches and overlapping functions lead to duplicated efforts and inefficient resource use.[66] Furthermore, cooperation between Nigerian authorities and international law enforcement agencies, such as Interpol, is often hindered by differing legal frameworks, language barriers, and political issues.[67]

Lack of Digital Forensic Capacity

One major challenge for Nigerian law enforcement in tackling cybercrime is the lack of capacity in digital forensics. Investigating crimes on social media requires advanced technical skills and specialized tools for extracting and analyzing digital evidence. Agencies like the NPF and EFCC often lack the necessary resources, training, and technology. Cybercriminals frequently use encrypted communication and sophisticated techniques to conceal their activities, making it essential to have specialized forensic tools, which Nigerian authorities struggle to access. This is made worse by the shortage of trained personnel in digital forensics among the judicial officers.

Jurisdictional Issues with Transnational Social Media Companies

Enforcing Nigerian cybercrime laws is hindered by jurisdictional challenges posed by transnational social media companies such as Meta (Facebook, Instagram, WhatsApp), X, and TikTok. These platforms operate under foreign laws, which makes compliance with Nigerian regulations voluntary. As a result, Nigerian law enforcement faces difficulties in accessing user data and removing harmful content, as they must navigate complex legal processes. Additionally, social media companies typically require a court order to disclose user data, complicating and slowing down the enforcement process.

Public Distrust in Law Enforcement

Public distrust in law enforcement in Nigeria hinders efforts to combat cybercrime. Many Nigerians see police as ineffective and corrupt, leading to reluctance in reporting cybercrimes, especially in cases like romance scams or blackmail. Victims often feel shame about their situations.[68] Additionally, a lack of public education about online risks contributes to the perception that cybercrime is less serious than traditional crime.

Underreporting Due to Stigma or Fear of Reprisals

A significant challenge in combating social media-facilitated cybercrime is the underreporting by victims. Many, especially those affected by romance scams, cyberstalking, and blackmail, hesitate to report incidents due to fear of stigma or retaliation. For instance, victims of romance scams may feel embarrassed, while those facing cyberstalking worry about additional harassment. This issue is worsened by the lack of victim support within law enforcement. Many victims are unaware of where to seek help, and even when they do, ineffective redress mechanisms lead to a perception that police are unhelpful or untrustworthy.[69]

5. Conclusion and Recommendations

The rapid growth of social media in Nigeria, while beneficial for communication, has led to a significant increase in cybercrimes like internet fraud and cyberbullying. Many of these crimes go unreported due to stigma, anonymity, and jurisdictional problems. Although laws exist (e.g., the Cybercrimes Act 2015), enforcement is hampered by weak coordination among agencies and a lack of technical expertise. Key agencies like the Police and EFCC are working on the issue, but effectively addressing it requires better funding, training, and international collaboration to enhance Nigeria's institutional capacity. The rise of cybercrime via social media in Nigeria necessitates a comprehensive approach to tackle the issue. Our key recommendations include the following:

Strengthening Legal Frameworks: Update existing laws, like the Cybercrimes Act 2015, to cover new cybercrime methods such as deepfakes and phishing.

Cybersecurity Education: Implement ongoing digital literacy and awareness campaigns for vulnerable groups, enabling them to recognize and avoid cyber threats.

Partnerships with Social Media Companies: Collaborate with platforms like Meta and TikTok to enhance information sharing for combating cybercrime.

Capacity Building for Law Enforcement: Provide funding and training for agencies like the Nigeria Police Force Cybercrime Unit to improve investigation capabilities.

Inter-agency and International Cooperation: Establish a national cybercrime task force for better coordination with domestic and international entities.

Promotion of Ethical Use of Social-Media: Encourage civil society and religious organizations to advocate for responsible social media use among youth.

Centralized Reporting System: Create a user-friendly online platform and hotline for reporting cybercrime incidents.

---

[65]M. Ibrahim and A. Ogunleye, 'The Role of NITDA in Nigeria's Cybersecurity Development: A Critical Appraisal' [2022] *Nigerian Journal of Law and Innovation (*6) 121.

[66] Ajayi (n 17) 87.

[67]C. Okeke, 'Jurisdiction and Social Media Compliance in Nigeria's Cybercrime Enforcement' [2023] *Nigerian Law and Digital Society Review* (15) 89.

[68]C. Ugochukwu, 'Institutional corruption is driving internet crimes in Nigeria' (11 June 2024) <https://www.thecable.ng/institutional-corruption-is-driving-internet-crimes-in-nigeria/?utm_source=chatgpt.com> accessed 28 March 2025.

[69] Ajayi (n 17) 91.