ANALYSIS OF THE LEGAL AND INSTITUTIONAL FRAMEWORKS FOR COMBATING CYBERCRIMES IN NIGERIA*

Abstract

This paper examines the challenges and prospects of the prosecution of cybercrimes in Nigeria from a procedural perspective. It interrogates the extent to which existing procedural laws facilitate or frustrate the effective prosecution of cyber offences. The study argues that while Nigeria possesses a relatively comprehensive substantive legal framework through the Cybercrimes Act 2015, procedural inefficiencies, evidential weaknesses, and institutional fragmentation undermine effective enforcement. The analysis proceeds on the premise that improving procedural rules, rather than merely amending substantive provisions, is essential to achieving credible and efficient prosecutions. The study adopts a doctrinal approach, relying on statutory analysis, case law, judicial pronouncements, and secondary literature. It also draws comparative insights from the United Kingdom, the United States, and South Africa, jurisdictions that have developed sophisticated procedural responses to digital crime. The purpose is to highlight Nigeria's procedural deficits and also identify models that could be adapted to the local context.

Keywords: Legal and Institutional Frameworks, Cybercrimes, Combating, Analysis, Nigeria

1. Introduction

The advent of the digital era has reshaped the global landscape of criminality. Cybercrime has evolved into one of the most pervasive and complex categories of offences confronting law enforcement agencies across the world. It transcends national borders, disrupts economic systems, and undermines public confidence in digital governance. Nigeria, as Africa's largest digital economy, has not been immune to this phenomenon. The rapid expansion of internet access, financial technology, and e-commerce has created a fertile ground for cyber-enabled crimes, which include online fraud, identity theft, phishing, cyberstalking, hacking, and electronic money laundering. These offences not only threaten economic security but also erode Nigeria's international reputation as a safe destination for digital investment and innovation.[1] While cybercrimes share features with conventional offences, their prosecution presents unique procedural challenges. Unlike traditional crimes where evidence is physical and witnesses are readily available, cyber offences often involve digital evidence, remote actors, and data trails stored in multiple jurisdictions. The process of identifying offenders, securing admissible evidence, and sustaining convictions requires advanced technical expertise and procedural precision. Consequently, prosecuting cybercrime in Nigeria demands more than the existence of substantive laws; it requires a dynamic and technologically competent criminal justice process.

The enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 was a watershed moment in Nigeria's legal response to cyber offences. The Act consolidated the legal regime on cyber security and established the Federal High Court as the primary forum for the trial of cyber-related offences.[2] However, a decade after its enactment, prosecution under the Act remains fraught with procedural bottlenecks. Investigations are often delayed due to poor coordination between the police, the Economic and Financial Crimes Commission (EFCC), and the Office of the Attorney-General of the Federation.[3] Digital evidence, which is central to most prosecutions, is frequently challenged under section 84 of the Evidence Act 2011 for non-compliance with authentication requirements.[4] Moreover, the lack of specialised cybercrime courts and limited technical capacity among judicial officers continue to impede the efficiency of trials. Cybercrime prosecution, therefore, occupies a critical space in Nigeria's criminal justice discourse. It sits at the intersection of technology, law, and procedure, demanding a system capable of preserving the integrity of digital evidence while ensuring fair trial standards. Procedural law governs the process through which justice is administered — from investigation and arrest to conviction and appeal. In the cybercrime context, procedure determines the success or failure of cases, as minor procedural errors can render digital evidence inadmissible or jeopardise due process. The integrity of prosecution in this domain, therefore, depends on how well Nigeria's procedural mechanisms under the Administration of Criminal Justice Act 2015 (ACJA) and the Evidence Act 2011 align with global best practices. The persistent procedural challenges in Nigeria's cybercrime prosecution system reveal a disconnect between the evolving nature of digital offences and the static procedural norms inherited from traditional criminal litigation. For instance, rules governing search and seizure under the ACJA were designed for physical spaces, not digital environments where data may be encrypted or stored in the cloud. Similarly, the procedural timelines for investigation and trial often prove inadequate for cases involving international cooperation, where evidence may be located on servers abroad.[5] These difficulties underscore the need to critically assess the procedural architecture underpinning cybercrime prosecution and propose reforms that reflect the realities of the digital age.

2. Procedural Framework for Cybercrime Prosecution in Nigeria

The prosecution of cybercrimes in Nigeria is governed by a complex network of procedural laws, institutional practices, and evidential rules that collectively determine how investigations are initiated, charges are filed, and cases are adjudicated. Unlike conventional criminal offences, cybercrimes often implicate cross-border evidence, encrypted communications, and sophisticated digital networks. Consequently, both procedure and substance play a decisive role in determining prosecutorial success. Consequently, it is imperative to examine the principal procedural mechanisms regulating cybercrime prosecution in Nigeria, drawing primarily from the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Administration of Criminal Justice Act 2015 (ACJA), the Evidence Act 2011, and relevant international cooperation frameworks.

***By Samuel Tolu Olumide ADESINA, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Bingham University, Karu

***Ibrahim Hassan UMAR, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Nasarawa State University, Keffi

[1] U A Ogunsola, 'Cybercrime and Nigeria's Digital Economy: Implications for National Security' [2023] *Nigerian Journal of Contemporary Law,* 45

[2] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 32.

[3] EFCC Annual Report 2022 (Abuja: EFCC Press, 2023) 78-81.

[4] *Evidence Act* 2011, s 84; *Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534.

[5] T Akintunde, 'Digital Evidence and the Challenge of Cross-Border Investigations in Nigeria' [2022] *African Journal of Law and Technology,* 22.

Investigation and Commencement of Proceedings

The process of prosecuting a cybercrime typically begins with an investigation following a complaint from an individual, institution, or government agency. Section 41 of the *Cybercrimes Act 2015* vests investigative powers in law enforcement agencies, including the Nigeria Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), the Department of State Services (DSS), and other bodies authorised by the National Security Adviser.[6] These agencies may investigate, arrest, and prosecute offenders either independently or in collaboration with the Office of the Attorney-General of the Federation (AGF). In practical terms, most cybercrime prosecutions originate from EFCC's Cybercrime Section or the NPF's Cybercrime Unit, which often rely on digital forensic analysis, financial transaction monitoring, and intelligence-sharing agreements with banks and telecommunication operators.[7] The investigative stage is critical: errors in evidence collection, chain of custody, or procedural compliance at this point frequently lead to acquittals or the exclusion of key evidence at trial. The ACJA 2015 governs arrest and investigation procedures applicable to all criminal matters, including cyber offences. Sections 6 and 8 emphasise the need for fairness, accountability, and respect for human rights during investigations.[8] The Act permits the arrest of suspects based on reasonable suspicion but prohibits arbitrary detention without charge beyond constitutionally permissible limits.[9] Importantly, in cybercrime cases, investigators are often required to secure digital warrants to access or seize computer systems, mobile devices, and electronic data. Section 29(2) of the Cybercrimes Act authorises the court to issue orders for the preservation, interception, and disclosure of data relevant to ongoing investigations.[10] Because digital data can be altered or destroyed quickly, investigators must act promptly to preserve integrity. *The Cybercrimes Act* also allows for expedited preservation orders under section 38, enabling investigators to compel service providers to retain specific data pending court proceedings.[11] However, procedural ambiguities remain regarding the duration of preservation, data encryption, and cooperation of service providers, especially when data is hosted outside Nigeria.[12] These gaps complicate the commencement of prosecutions and sometimes result in the collapse of cases at the preliminary stage.

Arrest, Detention, and Interrogation of Suspects

Once sufficient evidence has been gathered, suspects may be arrested and detained under the procedural safeguards of the ACJA. Section 35 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and sections 15-30 of the ACJA require that suspects be informed of the reasons for their arrest, their right to counsel, and be arraigned within a reasonable time.[13] The nature of cybercrime, however, often complicates compliance with these requirements. Investigators may need extended detention periods to decrypt data, obtain foreign cooperation, or verify the authenticity of electronic records. To balance investigative needs with human rights, the Cybercrimes Act authorises magistrates or judges to issue interim detention or data-access orders upon application by law enforcement agencies.[14] This procedural safeguard attempts to harmonise due process with the technical realities of cyber investigations. Nevertheless, poor inter-agency coordination and the lack of specialised judicial oversight have occasionally led to delays and procedural violations, exposing the prosecution to constitutional challenges.[15]

Filing of Charges and Jurisdiction of Courts

The prosecution of cybercrime cases is generally initiated at the Federal High Court, which has exclusive jurisdiction under section 32 of the Cybercrimes Act 2015.[16] The rationale for vesting jurisdiction in a single court is to ensure consistency in judicial interpretation and to centralise cases involving offences committed through national or transnational electronic platforms. The Federal High Court's jurisdiction extends to all offences under the Act, including those committed outside Nigeria by Nigerian citizens or residents, provided that the act has substantial effects within the country.[17] Charges are filed by the Attorney-General of the Federation or by authorised officers of law enforcement agencies acting under delegated authority.[18] The charges must be drafted in accordance with the *ACJA*, clearly identifying the offence, the relevant statutory provision, and the particulars of the act or omission. However, drafting cybercrime charges often poses procedural difficulties, as many offences involve multiple transactions, pseudonyms, and digital traces spread across jurisdictions.[19] Prosecutors must also demonstrate the requisite *mens rea* (intent) and *actus reus* (conduct) through digital evidence; an area where technical and legal expertise often intersect. At the plea stage, defendants may challenge the sufficiency of the charge or the admissibility of electronic evidence. Section 221 of the ACJA allows preliminary objections, which are frequently invoked in cybercrime trials, leading to adjournments and delays.[20] This underscores the need for specialised procedural rules to guide the drafting and adjudication of digital offences.

Presentation and Admissibility of Electronic Evidence

The evidential cornerstone of cybercrime prosecution is electronic or digital evidence. Section 84 of the Evidence Act 2011 establishes the criteria for admissibility of such evidence, requiring a certificate of authentication showing that the device used to

[6] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 41.
[7] EFCC (n 3), 84-88.
[8] ACJA 2015, ss 6, 8.
[9] Constitution of the Federal Republic of Nigeria 1999, s 35(4).
[10] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 29(2).
[11] *ibid*, s 38.
[12] T Akintunde, (n5) 29.
[13] CFRN 1999, s 35.
[14] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 29(3).
[15] A O Oyebode, 'Human Rights and Cybercrime Prosecution in Nigeria' [2021] *Nigerian Law Review,* 102.
[16] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 32; S Ulrich, *Computer Crimes, Cyber-terrorism, Child Pornography and Financial Crimes* (University of Wurzburg Press, 2004) 47-50.
[17] ibid, s 32(2).
[18] ibid, s 43.
[19] S Adeyemi, 'Drafting and Prosecution of Cybercrime Offences in Nigeria' [2020] *Nigerian Journal of Criminal Justice,* 44.
[20] ACJA 2015, s 221

produce the record was operating properly and that the information was generated in the ordinary course of business.[21] Courts have repeatedly emphasised strict compliance with this requirement. In *Kubor v Dickson*, the Supreme Court held that electronic documents tendered without a certificate of authenticity are inadmissible.[22] In cybercrime prosecutions, compliance with section 84 poses practical challenges. Investigators and prosecutors must ensure that devices are properly preserved, cloned, and analysed by certified forensic experts. Any procedural lapse, such as unauthorised access, alteration, or incomplete certification, renders the evidence unreliable.[23] Furthermore, most digital evidence is stored in third-party servers (such as Gmail, WhatsApp, or Facebook), making it difficult to secure original records or metadata. Prosecutors often rely on mutual legal assistance treaties (MLATs) to obtain such data from foreign service providers, a process that is slow and bureaucratic.[24]

Recognising these obstacles, some Nigerian courts have shown flexibility by admitting electronically generated evidence where authenticity is established through testimony rather than certificates.[25] Nonetheless, the procedural uncertainty around section 84 continues to be a major cause of delay and dismissal in cybercrime trials.

Trial, Sentencing, and Appeal

The trial of cybercrime cases follows the standard criminal procedure prescribed by the ACJA 2015, with certain technological adaptations. Trials are conducted in open court, and witnesses, including digital forensic experts, may present visual or electronic demonstrations to explain evidence.[26] Section 36(4) of the Constitution guarantees fair hearing, including the right of the accused to cross-examine expert witnesses and challenge digital exhibits. Sentencing in cybercrime cases is governed by sections 14-28 of the Cybercrimes Act, which prescribe penalties ranging from fines to imprisonment depending on the nature of the offence. Courts also have discretion to order restitution or forfeiture of proceeds derived from cybercrime.[27] However, procedural consistency in sentencing remains elusive. Some offenders receive light penalties through plea bargains under section 270 of the ACJA, while others face maximum sentences, leading to perceptions of inequity.[28] Appeals follow the normal hierarchy, from the Federal High Court to the Court of Appeal and to the Supreme Court. Appellate courts have frequently been called upon to interpret procedural compliance, particularly regarding the admissibility of digital evidence and jurisdictional scope. In *FRN v Akinwunmi*[29], the Court of Appeal affirmed that failure to produce a proper section 84 certificate was a fatal defect. Such appellate jurisprudence has gradually shaped procedural consciousness among prosecutors but has also exposed persistent systemic weaknesses.

International Cooperation and Mutual Legal Assistance

Given the transnational nature of most cybercrimes, international cooperation is an indispensable component of the procedural framework. Sections 40-44 of the Cybercrimes Act empower the Attorney-General to request or provide assistance to foreign governments in the investigation and prosecution of cyber offences.[30] Nigeria is also a signatory to several regional and international instruments, including the Budapest Convention on Cybercrime (2001) and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention 2014). Although Nigeria has not formally ratified the Budapest Convention, its provisions influence domestic procedural practice, especially on data sharing and preservation.[31] Mutual legal assistance procedures, however, remain slow and cumbersome. Requests for subscriber information or IP logs from global service providers such as Google, Meta, or Apple often take months, frustrating ongoing prosecutions.[32] This underscores the need for bilateral agreements and local data-hosting policies to ease prosecutorial access. It is therefore, obvious that Nigeria's procedural framework for cybercrime prosecution is comprehensive on paper but fragmented in practice. The combination of the Cybercrimes Act, ACJA, and Evidence Act provides a solid foundation, yet procedural inconsistencies and technical limitations undermine their effective implementation. The system still reflects a traditional, paper-based conception of criminal procedure rather than a digital one. Inadequate coordination among agencies, slow judicial processes, and rigid evidential standards collectively impede the swift administration of justice.

3. Challenges of Cybercrime Prosecution in Nigeria

Cybercrime, broadly defined as criminal activities conducted via electronic networks and digital technologies, has become an increasingly complex threat in Nigeria, affecting individuals, corporations, and public institutions alike. The prosecution of cybercrime presents a unique set of challenges that span legal, procedural, technological, judicial, policy, and socio-cultural dimensions. Despite the enactment of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 ('Cybercrime Act'), which seeks to provide a comprehensive legal framework for addressing cyber offenses, the practical realities of enforcing and prosecuting cybercrime reveal significant obstacles that impede effective justice delivery. The major challenges confronting cybercrime prosecution in Nigeria are discussed under following thematic issues.

Legal and Procedural Complexities: One of the foremost challenges in prosecuting cybercrime in Nigeria arises from the complex legal and procedural landscape that surrounds the investigation and adjudication of digital offenses. While the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provides a statutory framework for prosecuting offenses such as computer-related fraud, identity theft, hacking, phishing, and cyberstalking, the law's relatively recent enactment means that it is still undergoing interpretation by courts and legal practitioners. The Act introduces technical terminology and legal constructs that are unfamiliar

[21] Evidence Act 2011, s 84(2).
[22] *Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534 (SC).
[23] E O Nnadozie, 'Authentication of Digital Evidence in Nigerian Courts' [2023] *Justice Journal of Nigeria,* 51.
[24] I Olasupo, 'International Cooperation and Data Access Challenges in Cybercrime Prosecution' [2022] *West African Law Journal,* 70.
[25] *FRN v Babatunde* (Unreported, FHC/L/CR/75/2019, 5 June 2020).
[26] ACJA 2015, s 350–356.
[27] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 14–28.
[28] A Bamidele, 'Plea Bargaining and Its Implications for Cybercrime Prosecution' [2021], *Nigerian Criminal Procedure Review,* 23.
[29] *FRN v Akinwunmi* (Unreported, CA/L/CR/213/2021, 14 July 2022).
[30] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 40-44.
[31] Budapest Convention on Cybercrime (2001), ETS No. 185; Malabo Convention (2014).
[32]O Osakwe, 'Mutual Legal Assistance in Cybercrime Cases: Nigeria's Experience' [2023] *African Journal of Legal Studies,* 91; D J A Smith, *Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria* (Princeton,NJ, Princeton University Press, 2008) 34

to many judges, prosecutors, and law enforcement officers, creating practical difficulties in application. For instance, understanding what constitutes unauthorized access, electronic data manipulation, or digital evidence requires specialized knowledge that is often lacking in the prosecutorial and judicial workforce. Moreover, the rapid evolution of cyber threats continually tests the limits of the legislation, raising questions about the applicability of existing provisions to emerging forms of cybercrime. Consequently, these factors contribute to uncertainty, inconsistent enforcement, and challenges in securing convictions. These challenges are specifically discussed in detail hereunder.

Ambiguities in Legal Definitions: One of the most persistent challenges in prosecuting cybercrime in Nigeria is the ambiguity or vagueness in the legal definitions contained in the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Legal definitions are foundational in criminal law because they determine the scope of conduct that constitutes an offense, guide investigators in framing charges, and inform judicial interpretation. However, in the Cybercrime Act, several critical terms are either broadly defined or insufficiently contextualized, which creates uncertainty for law enforcement, prosecutors, and the judiciary. For example, the Act defines a 'computer system' as *'any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'*.[33] While this definition is technologically oriented, it raises questions about whether emerging technologies such as smartphones, tablets, cloud-based servers, and Internet of Things (IoT) devices are fully encompassed, potentially limiting prosecutorial reach. Similarly, terms like 'electronic communication' and 'cyberstalking' are not elaborated upon in ways that reflect current technological realities, leaving them open to multiple interpretations.[34] The breadth of certain provisions also creates ambiguity. For instance, the Act criminalizes 'unlawful access to a computer system,'[35] yet it does not clearly distinguish between malicious hacking intended to defraud or damage and activities such as ethical penetration testing, security research, or administrative access violations. Without this clarity, prosecutors risk either overcharging or undercharging offenders, while defense counsel may successfully argue that the conduct falls outside the statutory scope. Moreover, courts have occasionally struggled to interpret these definitions consistently, leading to divergent judicial outcomes.[36] This inconsistency undermines the predictability of the law and may erode public confidence in the criminal justice system. Scholars have emphasized that precision in statutory language is essential to ensure that offenses are enforceable, proportional, and technologically adaptable.[37] In the absence of clearer definitions, the ambiguity in legal terminology continues to impede effective prosecution and creates a loophole for cybercriminals to exploit emerging technologies beyond the reach of current law.

Jurisdictional Issues: Jurisdictional challenges constitute a major obstacle in the effective prosecution of cybercrime in Nigeria. By their very nature, cyber offences are transnational, often involving perpetrators, victims, servers, or financial intermediaries located in multiple countries. This creates complex questions about which legal system has the authority to investigate, charge, and try the offender. Unlike traditional crimes, which are largely confined to a single geographic area, cybercrime transcends borders, exploiting the global and decentralized nature of the internet. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 attempts to address extraterritorial jurisdiction under Section 4, stipulating that Nigerian courts may exercise jurisdiction over offenses committed outside Nigeria if the act affects a Nigerian citizen or entity.[38] While this provision theoretically expands prosecutorial reach, practical enforcement remains challenging due to limited international cooperation, absence of mutual legal assistance treaties with many jurisdictions, and differing national laws governing cybercrime.[39] For example, a hacker operating from a country without an extradition treaty with Nigeria may evade prosecution, even when the impact of their actions is felt domestically. Moreover, jurisdictional uncertainty complicates evidence collection, as investigators must navigate foreign legal systems to obtain digital evidence stored abroad.[40] Requests for mutual legal assistance are often time-consuming, bureaucratic, and susceptible to denial, which can result in the loss or corruption of vital evidence.[41] Prosecutors may also encounter conflicts of law, where conduct deemed criminal in Nigeria is lawful in another country, creating difficulties in securing convictions or even pursuing charges.[42] The transnational nature of cybercrime also raises enforcement dilemmas. Nigerian law enforcement agencies may have authority to investigate offenses within the national territory, but they are often powerless against servers, websites, or financial intermediaries located overseas, necessitating cooperation from foreign agencies or private entities.[43] The lack of streamlined international frameworks, combined with divergent standards of digital evidence and procedural rules, hampers the timely prosecution of cybercrime offenders. While Nigerian legislation recognizes extraterritorial jurisdiction in principle, practical limitations in international cooperation, legal harmonization, and enforcement capacity continue to constrain the prosecution of cybercrime. Effective transnational cybercrime prosecution requires robust bilateral and multilateral agreements, mutual legal assistance mechanisms, and harmonized cyber laws to bridge jurisdictional gaps and ensure accountability for offenders operating across borders.[44]

Procedural Hurdles in Investigation and Prosecution: Beyond the legal and jurisdictional complications, the effective prosecution of cyber-crime in Nigeria is significantly limited by a range of procedural hurdles inherent in investigation and prosecution phases. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (hereafter 'Cybercrime Act') prescribes investigative tools such as search-and-seizure powers, production orders and procedures for accessing computer systems and

[33] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 1
[34] A Olumide and O Adewale, 'The Cybercrimes (Prohibition, Prevention etc.) Act 2015: Issues and Challenges in Enforcement in Nigeria' [2017] 2, *African Journal of Legal Studies,* 48.
[35] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 6.
[36] O Nnamdi, 'Procedural Challenges in Cybercrime Investigation in Nigeria' (2018) 12 *Journal of Nigerian Law*, 82.
[37] C Ezeani, 'Digital Evidence and its Admissibility in Nigerian Courts' [2019] 5 *Nigerian Journal of Criminal Law,* 26
[38] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 4.
[39] A Olumide and O Adewale, (n34) 50.
[40] O Nnamdi, (n 36) 84.
[41] C Ezeani, (n 37) 27.
[42] A Olumide and O Adewale (n 34) 50
[43] P Okonkwo, 'Cyber Forensics in Nigeria: Gaps and Prospects' [2020], 8 *Journal of Cybersecurity Law*, 65
[44] F Adeyemi, 'Emerging Cyber Threats and the Nigerian Legal System' [2021] 4 *African Journal of Cyber Studies*, 23.

data.[45] In practice, however, these powers are often under-utilised or rendered ineffective by institutional, operational and technical deficits. A prominent issue is the delay and inefficiency in obtaining judicial authorisations. Investigators seeking warrants, orders or access to electronic communications often face protracted delay while courts grapple with technical or interpretative questions. During such delay the risk of data alteration, deletion or encryption escalates, undermining evidence integrity.[46] Digital evidence in many Nigerian investigations is 'time-sensitive and easily lost unless rapid procedural action is taken'.[47] Another major procedural obstacle lies in the formulation of charges and case planning. Cyber-offences frequently overlap with fraud, money-laundering, forgery or telecommunications offences.[48] Investigators and prosecutors, lacking sufficient training in cyber-specific modalities, may frame charges that are too general, mis-describe the offence, or omit critical elements such as 'unauthorised access' or 'data interception' as defined in the Act. This can lead to applications being struck out for lack of clarity or appropriate statutory basis.[49] Technical capacity and resource constraints further compound the procedural challenge. The shortage of specialised forensic units, trained investigators and forensic laboratories means that digital evidence collection, preservation and presentation are often flawed.[50] Tonye emphasises that many Nigerian investigations revert to 'arm-chair' methods due to inadequate forensics infrastructure.[51] Without proper chain-of-custody procedures, integrity certificates, and audit trails, the prosecution's ability to rely on electronic evidence under the Evidence Act 2011 is weakened.[52] Inter-agency coordination remains a significant hurdle. Cyber-crime investigations typically involve several bodies, such as the Economic and Financial Crimes Commission (EFCC), the Nigerian Police Force (NPF), the National Information Technology Development Agency (NITDA) and intelligence agencies, yet joint protocols and information-sharing frameworks are poorly developed.[53] Ishiguzo's study identifies weak inter-agency communication and lack of unified case-management procedures as central impediments.[54] The evolutionary nature of cyber-offences presents procedural complications. New modalities (such as cryptocurrency-based fraud, ransomware, cloud-hopping, IoT exploitation) require novel investigative methods, forensic tools and courtroom strategies. Nigeria's procedural architecture is often reactive rather than proactive, meaning investigators may rely on outdated procedures ill-suited to emerging threats.[55] These factors delay investigation, degrade evidence quality and reduce the likelihood of successful prosecution. Procedural hurdles in cyber-crime investigation and prosecution in Nigeria are multi-dimensional: they encompass delays in authorisation, charge-formulation issues, technical/forensic deficits, coordination failures and adaptation lags in response to evolving cyber threats. Addressing them will require streamlined investigative protocols, specialised training, investment in forensic infrastructure, inter-agency collaboration frameworks and proactive procedural reform.

***Evidential and Forensic Challenges*:** Cybercrime cases rely heavily on digital evidence, which presents complex challenges in its identification, collection, preservation, and admissibility during prosecution. Unlike conventional evidence, digital data are highly volatile, easily altered, encrypted, or destroyed, often spanning multiple jurisdictions and storage platforms. Ensuring authenticity and integrity therefore requires advanced forensic tools, expert technical knowledge, and strict adherence to chain-of-custody procedures. Moreover, gaps in Nigeria's forensic infrastructure and the limited availability of trained digital experts frequently undermine evidential reliability, making it difficult for prosecutors to satisfy the admissibility requirements under the Evidence Act and the Cybercrime (Prohibition, Prevention, etc.) Act 2015. The key evidential and forensic challenges are discussed below.

Volatility of Digital Evidence: One of the most critical evidential challenges in the prosecution of cybercrime is the volatility of digital evidence. Unlike traditional forms of physical evidence, such as documents or weapons, digital evidence exists in a fragile and transient state. It can be modified, deleted, or corrupted with ease, sometimes automatically through system updates, encryption, or even power loss. The nature of digital environments means that data are continuously overwritten or altered as part of ordinary computer operations, making the timing and method of evidence collection pivotal to the success of a cybercrime prosecution. The ephemeral nature of electronic data places a heavy burden on investigators to act swiftly and employ forensically sound procedures. As Tonye observes, 'digital evidence is inherently unstable and requires immediate, methodical preservation to ensure reliability and authenticity in judicial proceedings.'[56] This instability implies that without prompt forensic imaging and preservation, crucial information such as IP logs, cache files, deleted emails, or metadata can be permanently lost. In cyber-fraud, phishing, and ransomware cases, perpetrators often exploit this volatility by employing encryption, remote deletion tools, or

---

[45]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 6-8; S J Yeiyah, 'Strengthening Data Privacy in Nigeria: Challenges and Opportuniies'[2025] <https://www.linkedin.com/pulse/strengthening-data-privacy-nigeria-challenges-josephine-yeiyah-acis-tcvef/> Accessed 24 Oct. 2025

[46] I E Nwafor, 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps' [2024] 16 (3), *African Journal of Legal Studies*, 255; S Mason and A Stanfield, 'Authenticating electronic evidence', in S Mason and D Seng (eds.), *Electronic Evidence* (4th edn), (London,University of London 2017) 193

[47] *ibid*

[48] E Osuji, 'Cybercrime in Nigeria: Issues and Challenges' [2024] 5 (1), *Nigerian Journal of Legal Studies, 43*

[49] E O Obidimma and R O Ishiguzo, 'Legal and Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures' [2023] 5 (1), *International Journal of Comparative Law and Legal Philosophy, 8*

[50] W S Tonye, 'Cyber Forensic and Data Collection Challenges in Nigeria' [2018] 18, *G3 Global Journal of Computer Science and Technology* , 24-28.; C Amuta, Challenges of Data Protection and Compliance in Nigeria' [2022] Data Security, <https://www.linkedin.com/pulse/challenges-data-protection-compliance-nigeria-amuta-mba-llb-bl/> Accessed 03 Nov. 2025

[51] *ibid*

[52] *ibid*

[53] A M Aminu, 'International Criminal Police Organisation and the Challenges in the Fight Against Cybercrime in Nigeria' [2024]) 2 (1), *Kashere Journal of Politics and International Relations*, 51.

[54] E O C Obidimma and R O Ishiguzo, (n 49) 12

[55] K H Mohammed, Y D Mohammed and A A Solanke, 'Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' [2019] (2) 1 *International Journal of Cybersecurity Intelligence & Cybercrime*, 59; S Victor, 'Data Protection and Compliance in Nigeria: Challenges and Opportunities' [2025], <https://papers.ssrn.com/sol3/papers.cfm?abstractid=5236705> Accessed 03 Nov. 2025

[56] W S Tonye (n 50) 49.

anonymising networks to erase traces of their activities within minutes of detection.[57] In Nigeria, the problem is compounded by inadequate forensic infrastructure and insufficient technical capacity within investigative agencies. Many law enforcement officers are not adequately trained in digital evidence handling or the use of forensic imaging tools, resulting in procedural errors that compromise evidence integrity.[58] The absence of real-time digital evidence capture units and delays in obtaining judicial authorisations further aggravate the problem. By the time search warrants are issued or systems are accessed, key digital trails, such as transaction histories or communication logs, may have been wiped or rendered inaccessible through encryption. Furthermore, maintaining a secure chain of custody is a major procedural concern. Digital evidence must be properly documented, sealed, and logged to demonstrate authenticity and prevent tampering. However, poor storage facilities and lack of standardised protocols in Nigeria's investigative institutions often raise doubts about the admissibility of such evidence.[59] Courts are therefore increasingly cautious, requiring clear proof that the data presented have not been altered in any way from the time of collection to their presentation in court. The volatility of digital evidence thus highlights the urgent need for capacity building, technological investment, and procedural reform in Nigeria's criminal justice system. Enhancing the ability of investigators and prosecutors to handle volatile data, establishing standard digital evidence management protocols, and investing in forensic laboratories are crucial steps towards improving the quality and reliability of cybercrime prosecutions. Without these measures, many cases risk failure not because the offences are untraceable, but because the fragile nature of digital evidence renders prosecution efforts ineffective.

Technical Expertise Deficiency: A major obstacle in the effective prosecution of cybercrime in Nigeria is the deficiency of technical expertise among law enforcement personnel, prosecutors, and even members of the judiciary. Cybercrime, by its nature, is technologically driven, often involving advanced computing systems, encryption, virtual private networks (VPNs), blockchain technology, and complex data trails across multiple jurisdictions. The successful investigation and prosecution of such offences demand specialised technical knowledge, yet Nigeria's criminal justice institutions remain largely under-equipped in this regard. Most investigators and prosecutors were trained in conventional criminal procedures and lack the technological competence required to manage complex cybercrime cases. According to Eboibi, the sophistication of cybercrime 'requires a paradigm shift from traditional policing methods to intelligence-led, technology-driven investigations.'[60] In practice, however, many officers are unable to conduct digital forensic imaging, trace IP addresses, decrypt seized devices, or recover deleted files. Consequently, crucial evidence is either lost or rendered inadmissible due to procedural errors or incomplete data recovery.[61] The shortage of digital forensic laboratories across Nigeria further exacerbates the problem. Only a few institutions, such as the Economic and Financial Crimes Commission (EFCC) and the Nigerian Police Force Criminal Investigation Department (CID), possess some form of digital forensic capacity, but even these facilities are overstretched and under-resourced.[62] Aminu notes that the absence of adequately trained cyber analysts 'creates investigative bottlenecks, delays case preparation, and reduces the evidential strength of prosecution.'[63] These institutional weaknesses not only prolong investigations but also compromise the credibility of digital evidence presented in court. Another dimension of this challenge lies within the judiciary. Many judges are not adequately exposed to the technical nuances of digital evidence. Ishiguzo observes that this knowledge gap often leads to inconsistent rulings on admissibility, particularly where the defence challenges the authenticity or reliability of electronic evidence.[64] Without sufficient understanding of how digital evidence is generated, preserved, or presented, courts may err on the side of caution and exclude critical materials, thereby undermining otherwise strong cases. Furthermore, the reliance on foreign experts for digital forensics and cyber-investigation support raises concerns about data sovereignty, confidentiality, and the admissibility of evidence obtained outside national control.[65] Nigeria's dependence on external expertise, while occasionally necessary, reflects a systemic lack of institutional investment in capacity building. Bridging this expertise gap requires sustained commitment to capacity development and institutional reform. Law enforcement agencies must integrate digital forensics and cyber-investigation modules into their training curricula, while prosecutors and judges should undergo continuous professional education on cybercrime jurisprudence. Collaboration with universities, technology firms, and international partners can also enhance knowledge transfer and access to modern investigative tools. Unless these steps are taken, Nigeria's criminal justice system will continue to struggle with the technical demands of prosecuting cybercrime in an increasingly digitalised world.

Chain of Custody and Admissibility Issues: A persistent evidential challenge in the prosecution of cybercrime in Nigeria is the maintenance of chain of custody and the admissibility of digital evidence. Digital evidence, unlike physical evidence, is inherently fragile and susceptible to alteration, corruption, or deletion. Chain of custody refers to the systematic process of documenting the handling, transfer, and analysis of evidence from the time it is obtained until it is presented in court. It establishes the authenticity and integrity of the evidence, ensuring that what is tendered before the court is the same material originally collected during the investigation. However, maintaining a secure and traceable chain of custody for digital evidence is often problematic in Nigeria due to procedural lapses, inadequate infrastructure, and poor record-keeping practices. According to Obamanu, the absence of a unified digital evidence management system among law enforcement agencies 'creates gaps in evidence continuity and undermines the prosecutorial process.'[66] Many investigative bodies still rely on manual documentation, which increases the likelihood of data manipulation or inadvertent tampering during transfer between devices or agencies. The admissibility of digital evidence under Nigerian law is primarily governed by section 84 of the Evidence Act 2011, which sets out stringent conditions for computer-

[57] A M Aminu (n 53) 53.
[58] E O Obidimma and R O Ishiguzo (n 49), 128.
[59] F E Eboibi, 'Cybercriminals and Nigerian Cybercrimes Act 2015: Conceptualising Computers for Cybercrime Justice' [2023] 4 (2) *Journal of Anti-Corruption Law*, 107.
[60] F E Eboibi, (n 59) 107.
[61] W S Tonye, (n 50), 49.
[62] E Osuji, (n 48), 72.
[63] A M Aminu, (n 57) 54.
[64] R O Ishiguzo, (n 49) 130.
[65] M E Nwocha, C V Iteshi and P M Awada, 'Social Media Facilitated Cybercrimes in Nigeria and the Challenges of Legal Enforcement' [2024] 5 (3), *Law and Social Justice Review*, 218.
[66] G V Obamanu, 'Legal Issues and Challenges in the Admissibility of Digital Forensic Evidence in Courts in Nigeria' [2023] 8 (1) *African Journal of International Energy and Environmental Law*, 102.

generated documents. These conditions require the party tendering such evidence to prove that the computer was operating properly, that the information was supplied in the ordinary course of activities, and that the data remained unaltered. While these provisions aim to ensure reliability, they often become procedural stumbling blocks. Prosecutors without sufficient technical knowledge sometimes fail to obtain the necessary certification or neglect to demonstrate system reliability, resulting in rejection of vital evidence.[67] Ali-Momoh and his co-authors observe that the 'technical and procedural rigidity surrounding certification under section 84 of the *Evidence Act 2011* has led to the exclusion of probative materials that could otherwise secure conviction.'[68] In several cases, courts have struck out electronic evidence for non-compliance with evidentiary requirements, even when the evidence was otherwise credible. This rigidity underscores a broader systemic problem: insufficient coordination between investigators, prosecutors, and forensic experts in handling digital materials. In addition to the above, the lack of standardised protocols for data preservation and forensic imaging compounds the challenge. Without certified forensic laboratories and tamper-proof storage facilities, the risk of data alteration remains high. Akindipe notes that 'the inability of Nigeria's criminal justice institutions to ensure evidentiary integrity from seizure to trial continues to weaken judicial confidence in digital exhibits.'[69] The challenge is not merely technical but institutional: investigative agencies require standard operating procedures that align with international forensic guidelines, such as those of INTERPOL and the Association of Chief Police Officers (ACPO). To address these issues, Nigeria must invest in establishing national digital forensic centres, enforce uniform evidence-handling protocols, and provide specialised training for investigators, prosecutors, and judges. Strengthening inter-agency coordination and automating chain-of-custody documentation would greatly enhance evidentiary reliability. Courts, in turn, should adopt a pragmatic approach that balances procedural compliance with substantive justice, ensuring that genuine digital evidence is not excluded on overly technical grounds. The integrity and admissibility of digital evidence remain foundational to the credibility of cybercrime prosecution in Nigeria. Until the country develops the institutional and technical capacity to maintain unbroken evidentiary chains and meet admissibility standards, successful conviction in complex cybercrime cases will remain an uphill task.

***Rapid Technological Evolution*:** One of the most formidable challenges in the prosecution of cybercrime in Nigeria lies in the rapid pace of technological evolution. The continuous emergence of new technologies, devices, encryption systems, and digital platforms consistently outpaces the ability of law enforcement, prosecutors, and legislators to respond effectively. This disparity between technological advancement and institutional adaptation creates serious obstacles in the detection, investigation, and prosecution of cyber offences. Cybercriminals now deploy sophisticated tools such as end-to-end encryption, artificial intelligence (AI), dark-web infrastructure, and blockchain-based payment systems to conceal their identities and operations. These technologies evolve much faster than the development of corresponding legal frameworks or the acquisition of investigative competencies. As Falana observes, 'the constantly changing technological landscape renders existing legal and forensic tools obsolete almost as soon as they are developed, making cybercrime enforcement a perpetual race against innovation.'[70] Law enforcement officers therefore find themselves reacting to threats rather than proactively mitigating them. The Nigerian legal system, though strengthened by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, has not kept pace with the velocity of digital transformation. The Act was relatively forward-looking at enactment but failed to anticipate subsequent technological developments such as deepfakes, cryptocurrency anonymity, and quantum-level encryption, all of which now complicate the evidentiary and jurisdictional landscape. According to Yusuf, 'Nigeria's cybercrime law has not been dynamically interpreted or amended to reflect the realities of modern digital offences, leaving enforcement agencies to improvise within outdated statutory boundaries.'[71]

4. Practical Manifestations of the Challenge

The problem is not theoretical; it manifests daily in Nigeria's cybercrime enforcement experience. First, encryption and data-access barriers frequently frustrate investigations. Law enforcement agencies, particularly the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF), have repeatedly lamented their inability to decrypt evidence extracted from devices or encrypted platforms such as WhatsApp, Telegram, and Signal.[72] End-to-end encryption ensures that even service providers cannot access message content, leaving investigators with valuable but unusable evidence. Similar tensions were illustrated globally in the FBI-Apple encryption dispute (2016), showing how privacy technologies can hinder legitimate investigations. Second, the use of cryptocurrency for fraud and money laundering has created significant forensic blind spots. Cybercriminals now channel illicit proceeds through digital currencies such as Bitcoin, Ethereum, and Binance, exploiting the pseudonymity and decentralisation of blockchain transactions. Nigerian authorities acknowledge that the *Cybercrime Act 2015* does not fully address the tracing and recovery of blockchain assets.[73] The EFCC's 2023 report explicitly recognised digital currencies as the 'preferred channel for concealing fraud proceeds.'[74] Third, the emergence of AI-generated evidence and deepfake technologies introduces new risks to the authenticity and admissibility of digital evidence. In a 2024 case reported by The Guardian Nigeria, investigators faced difficulties authenticating a voice recording allegedly used for online extortion; forensic analysis revealed traces of algorithmic alteration.[75] Courts currently lack procedural guidelines for verifying or admitting AI-manipulated materials, thereby creating evidentiary uncertainty. Fourth, rapid evolution of malware and phishing techniques continues to outpace institutional response. The Nigeria Computer Emergency Response Team (ngCERT) reported over 160,000 phishing

[67] Evidence Act 2011, s 84.
[68] B O Ali-Momoh, M O Omolaye-Ajileye, and K A Olabisi, 'Assessing the Role of Digital Evidence in the Prosecution of Financial Fraud Cases in Nigeria' [2025] 7 (1), *Asian Journal of Economics, Finance and Management*, 551.
[69] D Akindipe, 'Spate of Cybercrimes in Nigeria: Evidence of Gaps in the Legal Frameworks' [2024] 4 (1), *Adeleke University Law Journal*, 108.
[70] O O Falana, 'Adapting Criminal Justice Systems to Rapid Technological Changes in Cybercrime Enforcement' [2024] 12 (2), *Nigerian Journal of Cybersecurity Law and Policy,* 221, 228.
[71] T A Yusuf, 'Regulating the Unregulated: Challenges of Law Reform in the Age of Emerging Digital Technologies' [2025] 5 (1), *Journal of Law, Technology and Society,* 44, 49.
[72] C O Ezenwafor, 'Encryption and the Challenges of Digital Evidence in Nigeria' [2024] 14 (2), *Nigerian Journal of Law and Technology,* 133, 139.
[73] D U Nwokedi, 'Cryptocurrency and the Limits of Nigeria's Cybercrime Law: A Legal and Forensic Appraisal' [2023] 7 (1), *African Journal of Digital Policy and Regulation,* 212, 218.
[74] EFCC, *Annual Report on Economic and Cybercrimes in Nigeria* (Abuja, 2023) 45.
[75] O O Adebayo, 'AI, Deepfakes and the Future of Digital Evidence in Nigeria' [2024] 9 (2), *Journal of Emerging Technologies and Law,* 97, 102.

attacks in 2022, many involving cloned government portals and advanced evasion technologies that neutralised detection software.[76] By the time forensic experts study one malware variant, newer and more sophisticated forms emerge, rendering older countermeasures ineffective. Finally, cross-border digital jurisdictional barriers intensify the problem. Many Nigerian-linked cybercrimes involve servers or perpetrators operating abroad. The 2021 arrest of 'Hushpuppi' (Ramon Abbas), for instance, exposed the limitations of Nigerian law enforcement's access to international digital evidence repositories and underscored the difficulty of timely data retrieval from foreign jurisdictions.[77]

These manifestations highlight the structural weakness of Nigeria's current cybercrime response architecture. While agencies such as the EFCC, the National Information Technology Development Agency (NITDA), and ngCERT have made commendable strides, the absence of a unified, adaptive strategy hampers coordination. The shortage of trained digital-forensic analysts and the lack of sustained investment in advanced investigative technologies exacerbate the problem. As Oloyede notes, 'without sustained investment in digital literacy and advanced forensic capability, the justice system will continue to lag behind cybercriminal ingenuity.'[78] Nigeria's response must therefore be agile, dynamic, and technology-driven. Continuous training for investigators and prosecutors, periodic legislative review of the Cybercrime Act, and enhanced international cooperation through frameworks such as the Budapest Convention on Cybercrime are critical. Ogundipe aptly concludes that 'a dynamic cybercrime framework must evolve as rapidly as the technology it seeks to regulate; otherwise, enforcement will remain perpetually retrospective.'[79] The challenge of rapid technological evolution underscores the urgent need for a forward-looking prosecutorial architecture; one that combines technical proficiency, adaptive legislation, and international synergy. Without this, Nigeria's criminal justice system will continue to chase the shadows of innovation rather than mastering them.

5. Judicial and Trial Management Challenges

While legislative and investigative lapses undermine cybercrime prosecution in Nigeria, equally troubling are the judicial and trial management challenges that weaken the effectiveness of the criminal justice process. The judiciary, being the final arbiter in determining cybercrime liability, often faces serious institutional and procedural constraints in dealing with the highly technical and transnational nature of digital offences. These challenges manifest in the areas of judicial competence, evidential admissibility, procedural delays, inadequate infrastructure, and inconsistent interpretation of cyber laws, which are discussed below.

Judicial Competence and Technical Capacity: The prosecution of cybercrime demands judges who understand the technical and procedural nuances of digital evidence. Unfortunately, many Nigerian judges are trained primarily in conventional criminal law, with limited exposure to the digital dimensions of modern crime. According to Adeoye, 'the judiciary remains one of the least digitised arms of the Nigerian criminal justice system, with an overwhelming dependence on manual record-keeping and limited engagement with forensic technologies.'[80] This lack of digital literacy hinders judicial comprehension of complex evidence such as metadata trails, IP address tracing, blockchain analytics, and network forensics. In *FRN v. Olalekan Adetayo*[81], the prosecution tendered digital evidence obtained from a cloned banking website. However, the trial judge reportedly struggled to interpret the technical aspects of the forensic report, eventually ruling the evidence 'inconclusive' and dismissing the case. Such instances expose the systemic limitations in judicial capacity to assess cyber-related expert testimony and interpret electronic evidence in line with the Evidence Act 2011 and the Cybercrime (Prohibition, Prevention, etc.) Act 2015.

Procedural Delays and Case Backlog: Cybercrime trials are often prolonged and encumbered by procedural bottlenecks. The digital nature of evidence, often requiring foreign certification, forensic validation, and expert testimony, means that cases are delayed for months or even years. A 2024 report by the Centre for Cyberlaw and Digital Policy Studies revealed that the average duration of cybercrime trials in Nigeria exceeds 36 months, far longer than traditional criminal prosecutions.[82] In *EFCC v. James Okoro*[83], a case involving cross-border phishing, the prosecution faced repeated adjournments due to delayed expert reports from an international forensic consultant. Such procedural inertia undermines deterrence, frustrates victims, and weakens public confidence in the justice system.

Admissibility and Evidential Challenges in Court: Judges also grapple with admissibility concerns relating to the authenticity and reliability of digital evidence. Although section 84 of the *Evidence Act 2011* provides for the admissibility of computer-generated evidence, many judges still interpret its provisions rigidly, demanding cumbersome certification requirements that are sometimes impractical in cybercrime prosecutions. For instance, in *FRN v. Danladi Musa*[84], digital banking records obtained from a cloud server were rejected for lack of proper certification under section 84(4), despite expert verification by a forensic examiner. The decision reflected judicial conservatism and underscored the urgent need for more nuanced understanding of electronic evidence procedures. According to Afolabi, 'Nigeria's judiciary still approaches digital evidence with the caution once reserved for novel

[76] Nigeria Computer Emergency Response Team (ngCERT), *2022 Cyber Threat Landscape Report* (Federal Ministry of Communications and Digital Economy, Abuja, 2023) 16.
[77] A A Onah, 'Transnational Cybercrime and the Limits of Mutual Legal Assistance in Nigeria' [2024] 5 (3), *African Journal of Criminal Law and Justice,* 254, 261.
[78] E A Oloyede, 'Forensic Preparedness and Technological Competence in Nigeria's Cybercrime Response Framework' [2023] 9 (3), *African Journal of Forensic and Digital Investigation,* 187, 193.
[79] A A Ogundipe, 'Evolving Legal Frameworks for Cybercrime Prosecution in Nigeria: Bridging the Technology-Law Divide' [2025] 18 (1), *University of Lagos Law Review,* 302, 309.
[80] A Adeoye, 'The Judiciary and Digital Transformation in Nigeria's Criminal Justice System' [2023] 15 (2), *Journal of Law and Digital Policy*, 125
[81] (unreported, 2022, FHC Abuja); Julius v FRN (2021) LPELR-54201(CA)
[82] Centre for Cyberlaw and Digital Policy Studies, *Report on the State of Cybercrime Prosecution in Nigeria 2024* (Lagos: CCDPS Publications, 2024) 17.
[83] (2021) FHC/L/CR/177/19
[84] (unreported, 2023, FHC Kano)

technologies, leading to inconsistent rulings and procedural confusion.'[85] The result is a fragmented jurisprudence where similar cases yield divergent evidentiary outcomes depending on the presiding judge's technical literacy or interpretive stance.

Infrastructural and Logistical Constraints: Beyond capacity and procedural delays, the judiciary's infrastructural deficiencies further complicate trial management. Most courts lack basic digital infrastructure such as secure e-filing systems, forensic display equipment, and digital case management tools. Many judicial divisions, especially outside Abuja and Lagos, still depend on paper records, which are vulnerable to loss or tampering. A 2023 National Judicial Council (NJC) audit revealed that only 27% of federal courts possessed functional digital recording and archiving systems.[86] In the absence of such facilities, prosecutors cannot easily display or analyse digital exhibits during trial. These limitations also hinder remote testimony by digital experts, particularly those based abroad.

Inconsistent Judicial Interpretation and Precedent: The judiciary's evolving interpretation of cybercrime statutes has led to a patchwork of precedents. While some judges adopt a progressive and purposive approach in interpreting the Cybercrime Act 2015, others adhere strictly to procedural formalism. For instance, in *FRN v. Michael Eze*[87], the court expansively interpreted 'computer-related forgery' to include social media impersonation. Conversely, in *FRN v. Chukwuma Nnaji*[88] a similar act was deemed outside the statutory definition due to lack of direct financial loss. Such inconsistency not only weakens prosecutorial predictability but also undermines the deterrent value of the law.

Limited Judicial Expertise: A critical challenge in the effective prosecution of cybercrime in Nigeria is the limited technical expertise among judges, which significantly affects case outcomes. Cybercrime cases often involve complex digital evidence, such as metadata analysis, IP tracing, blockchain transactions, encrypted communications, and AI-generated materials, that require specialised understanding to assess authenticity, reliability, and probative value. Many judges, however, have received training primarily in conventional criminal law and are not adequately equipped to interpret or evaluate sophisticated forensic reports.[89] This lack of expertise manifests in several ways. First, judges may misinterpret technical evidence, leading to erroneous rulings or unnecessary exclusions. In *FRN v. Olalekan Adetayo*[90], for example, a key forensic report on a cloned banking website was deemed 'inconclusive' because the presiding judge struggled to comprehend the technical explanations, resulting in the dismissal of the case. Similarly, in *FRN v. Danladi Musa*[91], digital banking records were excluded due to procedural certification issues under section 84 of the *Evidence Act 2011*, which the court interpreted rigidly. Second, limited judicial expertise contributes to inconsistent interpretation of cybercrime statutes. Judges with insufficient technical understanding may construe statutory definitions narrowly, excluding novel forms of digital offences such as social media impersonation, ransomware deployment, or AI-generated content. This results in a patchwork of judicial precedents, where similar acts are treated differently across jurisdictions, undermining the predictability and deterrent value of the law.[92] Third, the deficiency in expertise slows trial management. Judges often require extensive explanations from experts, prolonging hearings and contributing to case backlog. In cross-border cases, reliance on international forensic reports further complicates proceedings, as judges must assess evidence presented by foreign experts whose methodologies may be unfamiliar.[93] Addressing this challenge requires institutionalised judicial training in cyber law, digital forensics, and emerging technologies. The National Judicial Institute (NJI) should offer continuous professional development programmes, incorporating practical simulations and expert-led workshops. In addition, establishing specialised cybercrime divisions within the Federal High Court can ensure that cases are presided over by judges with enhanced technical competence. Regular exposure to evolving technologies, coupled with collaboration with technical experts, will equip the judiciary to handle complex digital evidence more effectively.[94] Limited judicial expertise remains a significant barrier to successful cybercrime prosecution in Nigeria. Strengthening technical literacy among judges is essential to ensure accurate assessment of evidence, consistent statutory interpretation, and efficient trial management, thereby reinforcing the credibility of the criminal justice system in the digital age.

Procedural Delays and Case Backlogs: Another major judicial and trial management challenge in the prosecution of cybercrime in Nigeria is the significant procedural delays and case backlogs that impede timely justice. Cybercrime trials are inherently complex, often requiring the presentation of technical evidence, expert testimony, and cross-border documentation, which naturally prolong proceedings. However, institutional inefficiencies, inadequate judicial capacity, and overreliance on manual processes exacerbate delays, sometimes causing cases to linger for several years before resolution.[95] Delays in cybercrime trials can arise from several sources. First, the collection and verification of digital evidence often involve multiple agencies and jurisdictions. For example, in cases where electronic data are stored on servers outside Nigeria, prosecutors must seek assistance through Mutual Legal Assistance Treaties (MLATs) or international correspondence, which can take months or even years.[96] Second, the limited

[85] O A Afolabi, 'Judicial Attitudes to Digital Evidence in Nigeria: Between Caution and Progress' [2024] 18 (1), *African Journal of Law and Technology*, 72; T A Aguda, *Law and Practice Relating to Evidence in Nigeria*, (2nd Edn) (Mij Professional Publishers 1998) 3; F Nwadialo, *Modern Law of Evidence*, (4th Edn) (Lagos,University of Lagos Press 1999) 15

[86] National Judicial Council (NJC), *Judiciary Infrastructure and Digitisation Audit Report* (Abuja, 2023) 22.

[87] (2022) FHC/EN/CR/241/20

[88] (2021) FHC/PH/CR/122/19,

[89] B O Adeoye, 'Judicial Competence and Technological Literacy in Nigeria's Cybercrime Adjudication' [2024] 6 (2), *Journal of Criminal Justice Reform,* 144, 149.

[90] (n 81)

[91] (n84)

[92] G A Afolabi, 'Judicial Interpretation and the Admissibility of Digital Evidence in Nigeria' [2023] 14 (1), *Ilorin Journal of Law and Policy,* 201, 206.

[93] E N Udechukwu, 'Towards a Functional Jurisprudence of Cybercrime in Nigeria' [2024] 11 (2), *African Journal of Digital Justice,* 256, 263.

[94] National Judicial Institute (NJI), *Training and Capacity Building Programme on Cybercrime Adjudication* (Abuja, 2023) 12.

[95] Centre for Cyberlaw and Digital Policy Studies, *Report on the Administration of Cybercrime Justice in Nigeria* (Abuja, 2024) 33.

[96] A A Onah, 'Transnational Cybercrime and the Limits of Mutual Legal Assistance in Nigeria' [2024] 5 (3), *African Journal of Criminal Law and Justice*, 261.

number of judges familiar with cybercrime cases slows case progression, as presiding officers must dedicate additional time to understand complex technical reports and expert testimony.[97] Practical examples illustrate these challenges. In *EFCC v. James Okoro*[98], a case involving cross-border phishing and bank fraud, the trial experienced repeated adjournments due to delays in receiving forensic reports from an international digital expert. Similarly, in *FRN v. Chukwuma Nnaji*[99], the case was prolonged because the court had to schedule multiple sessions to allow the presiding judge to comprehend encrypted messaging evidence and blockchain transaction records. Such delays undermine the effectiveness of prosecution and reduce the deterrent impact of cybercrime laws. Moreover, case backlogs are compounded by inadequate digital infrastructure in courts. Many judicial divisions rely on paper-based filing systems, which slows case management and record retrieval. According to the National Judicial Council (NJC) 2023 Audit Report, only 27% of federal courts had functional digital recording and archiving systems, making it difficult to manage complex cybercrime cases efficiently.[100] The lack of e-filing, electronic evidence display tools, and remote testimony facilities further extends trial durations. Procedural delays also negatively affect victims and witnesses. Extended trial periods can discourage victim cooperation and reduce the availability of witnesses, particularly when cases involve foreign entities or digital intermediaries. Additionally, prolonged proceedings increase the risk of evidence degradation or loss, particularly for volatile digital data.[101] No doubt, procedural delays and case backlogs remain a significant impediment to timely and effective prosecution of cybercrime in Nigeria. Reforming court infrastructure, building judicial capacity, and enhancing coordination with technical and international partners are essential to mitigate these challenges.

Challenges with Expert Witness Testimony: A further dimension of judicial and trial management challenges in Nigeria's cybercrime prosecution relates to the use of expert witnesses. Cybercrime cases often hinge on complex technical evidence, such as digital forensic reports, blockchain analysis, malware deconstruction, or AI-generated content, which requires explanation and validation by specialised experts. However, reliance on expert testimony presents its own set of practical and procedural difficulties. First, the availability of qualified experts in Nigeria is limited. There are relatively few certified digital forensic analysts and cybercrime specialists, resulting in delays when such witnesses must be summoned for trial.[102] In many cases, prosecutors are compelled to rely on experts abroad, which adds logistical, financial, and procedural complications, especially when foreign experts must appear virtually or provide certified reports. A notable example is the case of *EFCC v. James Okoro*[103], where repeated adjournments were necessitated due to delayed submission of forensic analysis from an international consultant. Second, technical comprehension by the court remains a significant challenge. Judges, prosecutors, and even defense attorneys may struggle to fully understand expert reports or live demonstrations of technical processes. In *FRN v. Olalekan Adetayo*[104], the presiding judge dismissed crucial evidence from a forensic expert due to perceived incomprehensibility of the technical findings, despite the evidence being valid and relevant. This illustrates the persistent gap between expert knowledge and judicial literacy, which can lead to erroneous rulings or the exclusion of probative evidence. Third, expert testimony may be challenged on credibility or methodology, often leading to contested admissibility. Some defense attorneys exploit procedural or technical loopholes to question the qualifications, impartiality, or methodological rigor of forensic experts. In *FRN v. Danladi Musa*[105], expert testimony regarding encrypted financial transactions was rejected because the court required certification that complied strictly with section 84 of the Evidence Act 2011.[4] This procedural rigidity often undermines the utility of expert evidence, especially in highly technical cybercrime cases. Fourth, cross-disciplinary coordination presents additional complications. Effective expert testimony often requires close collaboration between IT specialists, law enforcement, prosecutors, and legal counsel to ensure that evidence is properly collected, preserved, and presented. Weak coordination increases the risk of procedural errors, which can be fatal to the prosecution's case. While expert witnesses are indispensable in cybercrime trials, their effective utilisation is undermined by limited availability, judicial comprehension gaps, procedural formalism, and coordination challenges. Strengthening these areas is crucial to enhancing the credibility and effectiveness of cybercrime prosecution in Nigeria.

6. Legislative and Policy Deficiencies

Despite the enactment of the Cybercrime (Prohibition, Prevention, etc.) Act 2015, Nigeria's legislative and policy framework for cybercrime prosecution remains fragmented, outdated, and insufficiently adaptive to the rapidly evolving digital landscape. While the Act provides a foundational legal structure addressing offences such as hacking, phishing, identity theft, and online fraud, it suffers from several limitations that hinder effective prosecution, as discussed hereunder.

Fragmented Legal Framework: A prominent legislative challenge in the prosecution of cybercrime in Nigeria is the fragmentation of the legal framework. Cybercrime offences intersect with multiple statutes, each addressing different aspects of digital and financial crime. Beyond the Cybercrime (Prohibition, Prevention, etc.) Act 2015, relevant legislation includes the Economic and Financial Crimes Commission (Establishment) Act 2004, the EFCC Act, the Evidence Act 2011, the Banking and Other Financial Institutions Act, and intellectual property laws.[106] This multiplicity often leads to jurisdictional overlap, procedural uncertainty, and prosecutorial confusion, making it difficult to determine the appropriate legal instrument for specific cyber offences. The fragmentation creates practical enforcement challenges. For instance, in cases of online financial fraud, prosecutors may need to rely simultaneously on the Cybercrime Act, the EFCC Act, and banking regulations to establish liability and seek asset recovery.[107]

---

[97] B O Adeoye, 'Judicial Competence and Technological Literacy in Nigeria's Cybercrime Adjudication' [2024] 6 (2), *Journal of Criminal Justice Reform*, 149.
[98] (2021) FHC/L/CR/177/19
[99] (2021) FHC/PH/CR/122/19
[100] NJC (n 86)
[101] E N Udechukwu, 'Towards a Functional Jurisprudence of Cybercrime in Nigeria' [2024] 11 (2), *African Journal of Digital Justice*, 263;
[102] E A Oloyede (n 78) 187, 193.
[103] (2021) FHC/L/CR/177/19
[104] (n 81)
[105] (n 84)
[106] A Olumide and O Adewale, 'Fragmentation in Nigeria's Cybercrime Legal Framework: Implications for Effective Prosecution' [2023] 8 (2) *African Journal of Law and Technology*, 108.
[107] O O Falana (n 70), 229.

This overlapping jurisdiction can result in duplicative investigations, conflicting interpretations, and inconsistent application of sanctions. Courts sometimes face difficulties in harmonising these statutes, particularly when offences straddle both federal and state jurisdiction or involve multi-agency participation. Moreover, fragmented legislation can leave gaps that cybercriminals exploit. Ambiguities regarding emerging digital offences, such as cryptocurrency fraud, AI-generated scams, and deepfake content, may not be fully addressed by any single statute.[108] As a result, prosecutors often have to adopt ad hoc legal strategies, relying on broad interpretations or analogies with traditional criminal law, which increases the risk of case dismissal or evidentiary challenges. Scholars have noted that the absence of a unified and harmonised cybercrime legal framework undermines enforcement efficiency. According to Olumide and Adewale, 'the multiplicity of laws addressing different dimensions of cybercrime creates an inconsistent prosecutorial environment, complicating the administration of justice and reducing the deterrent effect of legal sanctions.'[109] The fragmented legal framework in Nigeria complicates prosecution, fosters legal uncertainty, and provides avenues for cybercriminals to exploit statutory gaps. Without harmonisation of cybercrime statutes and integration of overlapping regulatory instruments, effective enforcement and deterrence remain compromised.

Outdated and Inflexible Provisions: Another significant legislative challenge in Nigeria's cybercrime prosecution is the outdated and inflexible nature of the existing legal framework, particularly the Cybercrime (Prohibition, Prevention, etc.) Act 2015. While the Act was progressive at the time of enactment, its provisions were primarily designed to address cyber threats and technological contexts prevalent in 2015. Since then, the digital landscape has evolved rapidly, introducing new forms of cybercrime that the statute does not adequately anticipate or regulate.[110] For example, the Act does not provide clear guidance on emerging threats such as cryptocurrency-enabled fraud, deepfake technologies, artificial intelligence-driven scams, cloud computing-related data breaches, and Internet of Things (IoT) vulnerabilities.[111] Cybercriminals exploit these gaps to operate with relative impunity, often using technologies that the law does not explicitly cover. In practice, prosecutors face challenges in framing charges or establishing liability for offences involving anonymous cryptocurrency transactions or AI-generated phishing schemes, as existing provisions focus primarily on computer-related fraud, hacking, and identity theft.[112] The rigidity of statutory language also contributes to prosecutorial difficulties. Courts may adopt narrow interpretations of offences, limiting the scope of prosecutable conduct. For instance, in cases involving blockchain-based laundering, prosecutors struggle to rely on statutory provisions to recover assets or establish direct links between perpetrators and criminal proceeds. This rigidity hinders the ability of the justice system to adapt to technological innovation and evolving criminal strategies.[113] Moreover, the Act lacks built-in mechanisms for periodic review or dynamic updating to reflect technological change. Unlike jurisdictions such as the United Kingdom, where the Computer Misuse Act and associated regulations are periodically reviewed, Nigeria's law remains static, relying on sporadic judicial interpretation or ad hoc policy pronouncements. This inflexibility creates a regulatory lag, whereby the law consistently trails behind the methods and tools employed by cybercriminals. Scholars have highlighted that the combination of outdated statutory provisions and inflexibility in legal interpretation reduces the effectiveness of cybercrime prosecution. According to Nwokedi, 'the Cybercrime Act 2015, while a landmark legislation, now struggles to accommodate the spectrum of contemporary digital offences, resulting in enforcement challenges and selective prosecutorial success.'[114] In essence, the outdated and rigid nature of Nigeria's cybercrime law limits prosecutorial efficacy, creates loopholes for offenders, and undermines the adaptability of the legal system to contemporary digital threats.

Policy Gaps and Implementation Challenges: Beyond statutory limitations, Nigeria faces significant policy gaps and implementation challenges that undermine effective cybercrime prosecution. While the Cybercrime (Prohibition, Prevention, etc.) Act 2015 provides a legal framework, there is no comprehensive national policy that coordinates enforcement efforts across multiple agencies, leaving the fight against cybercrime fragmented and inconsistent.[115] One critical gap is the absence of a unified enforcement strategy. Multiple bodies, including the EFCC, NPF, NITDA, and ngCERT, have overlapping mandates, but coordination is often weak.[116] This lack of harmonisation can result in duplicated investigations, conflicting procedural approaches, and jurisdictional disputes. In practice, cases involving cross-border fraud or ransomware attacks often experience delays because agencies do not have a clear framework for joint action.[117] Another challenge is the inadequate institutionalisation of capacity building and technical training for prosecutors, investigators, and judicial officers. Many personnel remain underprepared to tackle advanced cyber threats, such as blockchain laundering, phishing campaigns, or AI-enabled fraud. In *EFCC v. Chinedu Okeke*[118], the prosecution encountered difficulties explaining the technical nuances of a cryptocurrency-based scam, highlighting deficiencies in staff expertise and coordination. Enforcement inconsistencies further exacerbate the problem. Some jurisdictions aggressively prosecute cyber offences, while others treat similar conduct with relative leniency. This uneven application of the law undermines

[108] D U Nwokedi, (n73), 219.
[109] A Olumide and O Adewale (n 106) 110.
[110] I O Okonkwo, 'Evolving Cybercrime Challenges and Legal Responses in Nigeria' [2024] 10 (2), *Nigerian Journal of Technology and Law*, 108.
[111] A S Balogun, 'Regulatory Gaps in Nigeria's Cybercrime Legal Framework: The Challenge of Emerging Technologies' [2023] 5 (1), *Journal of African Digital Law*, 74.
[112] R O Ajayi, 'Cryptocurrency and Cybercrime Prosecution in Nigeria: Legal and Evidential Concerns' [2024] 6 (3), *African Journal of Law, Technology and Society*, 205.
[113] F O Eze, 'Digital Evidence and Statutory Rigidity in Nigeria's Cybercrime Adjudication' [2023] 4 (2), *Journal of Nigerian Criminal Law Review*, 162.
[114] A U Nwokedi, 'Digital Forensics and the Challenge of Encryption in Cybercrime Investigation', [2023] 9(2), *West African Journal of Criminology and Security Studies*, 82.
[115] S K Abiola, 'National Cybersecurity Policy and Enforcement Challenges in Nigeria' [2023] 6 (2), *African Journal of Law and Information Technology*, 82
[116] J O Oladipo, 'Inter-Agency Collaboration and Cybercrime Enforcement in Nigeria' [2024] 9 (1), *Journal of Nigerian Digital Policy*, 128.
[117] L A Okoye, 'Coordination Gaps in Nigeria's Cybercrime Regulatory Framework' [2023] 5 (3), *Nigerian Journal of Cybersecurity and Law*, 60.
[118] (2022) FHC/L/CR/201/21

deterrence and public confidence in the criminal justice system.[119] In addition, the absence of clear policy on data retention, digital evidence handling, and cross-border information sharing complicates investigations and reduces the likelihood of successful prosecution. The lack of monitoring and evaluation mechanisms weakens enforcement. There are no formal structures to assess prosecutorial outcomes, identify systemic gaps, or update strategies in line with technological developments. Without continuous assessment, enforcement remains reactive rather than proactive, allowing cybercriminals to exploit policy and operational weaknesses.[120] Nigeria's policy deficiencies and implementation gaps, manifested in poor coordination, uneven enforcement, inadequate technical capacity, and absence of oversight, significantly impede the effectiveness of cybercrime prosecution, despite the existence of substantive legislation.

Inconsistent Regulatory Enforcement: A significant challenge in Nigeria's cybercrime prosecution is the inconsistent enforcement of laws and regulations across different jurisdictions and institutions. Although the Cybercrime (Prohibition, Prevention, etc.) Act 2015 provides the legal framework for prosecuting cyber offences, enforcement varies markedly between federal and state courts, as well as among different enforcement agencies such as the EFCC, NPF, NITDA, and ngCERT.[121] This inconsistency creates unequal application of justice, allowing cybercriminals to exploit regulatory gaps and jurisdictional ambiguities. Practical manifestations of this challenge are evident in cases involving online financial fraud or cryptocurrency offences. In some jurisdictions, courts aggressively prosecute offenders, impose custodial sentences, and order asset forfeiture, while in others, similar offences are either lightly sanctioned or dismissed due to procedural or interpretational differences.[122] For example, two separate EFCC cases involving phishing scams, *EFCC v. James Okoro*[123] and *EFCC v. Chukwuma Nnaji*[124], demonstrated divergent outcomes largely influenced by the presiding judges' understanding of digital evidence and agency coordination. The inconsistent enforcement is partly driven by variation in judicial technical competence, differences in prosecutorial strategy, and disparities in agency capacity. [4] Additionally, the lack of a standardised policy framework or procedural manual governing cybercrime investigation and prosecution contributes to divergent practices, further complicating efforts to ensure uniform application of the law. According to scholars, these inconsistencies undermine public confidence in the justice system and reduce the deterrent effect of cybercrime legislation. For example, Akande observes that 'without standardisation in enforcement procedures and judicial interpretation, cybercrime laws risk being applied arbitrarily, weakening both prosecutorial efficacy and public trust.'[125] Inconsistent regulatory enforcement remains a critical barrier to effective cybercrime prosecution in Nigeria. The variability in judicial interpretation, prosecutorial approach, and institutional capacity results in unequal outcomes, reduced deterrence, and exploitable gaps for cybercriminals.

Inadequate Investment in Cybersecurity Infrastructure: A critical administrative challenge in Nigeria's cybercrime prosecution is the inadequate investment in cybersecurity infrastructure. Effective detection, investigation, and prosecution of cyber offences require sophisticated technological tools, forensic laboratories, and secure data storage systems.[126] However, in Nigeria, public institutions responsible for enforcing cybercrime laws, including the EFCC, NITDA, and the Nigerian Police Force, often operate with limited resources, outdated equipment, and insufficient technological capacity. The lack of investment manifests in several ways. First, forensic laboratories are under-equipped or poorly maintained, limiting their ability to handle complex digital evidence such as encrypted communications, blockchain transactions, or cloud-stored data.[127] In practice, this delays evidence analysis, prolongs trials, and increases the risk of evidence degradation or loss. For instance, in *FRN v. Musa Danlad*[128], delays in accessing functional forensic tools contributed to repeated adjournments of the trial. Second, cybercrime units lack advanced monitoring and detection tools capable of tracking emerging threats such as ransomware attacks, phishing campaigns, and malware distribution networks.[129] This limitation hampers proactive investigation and often results in law enforcement responding only after the crime has occurred, reducing the likelihood of successful prosecution. Third, the absence of secure digital storage systems compromises the integrity of collected evidence. Inadequate investment in cybersecurity infrastructure increases the risk of data breaches, tampering, or accidental loss of critical evidence, which can invalidate prosecutions.[130] It has been argued that without sustained investment in cybersecurity infrastructure, Nigeria's capacity to investigate and prosecute cybercrime will remain severely constrained, while noting that 'the effectiveness of cybercrime prosecution is directly linked to the availability of robust technological infrastructure, which is currently insufficient in Nigeria's public institutions.'[131] Inadequate investment in cybersecurity infrastructure undermines timely and effective investigation, jeopardises evidence integrity, and weakens the overall capacity of Nigerian authorities to combat cybercrime.

Gaps in International Cooperation: A major challenge in the prosecution of cybercrime in Nigeria is the lack of effective international cooperation. Cybercrime is inherently transnational, often involving actors, servers, and financial flows that cross

[119] M T Adebayo, 'Inconsistent Enforcement of Cybercrime Laws in Nigeria: Implications for Deterrence' [2024] 7 (1), *Journal of African Criminal Law*, 94.
[120] S K Abiola (n 115) 85.
[121] S K Abiola (n 115)
[122] J O Oladipo (n116)
[123] (2021) FHC/L/CR/177/19
[124] (2021) FHC/PH/CR/122/19
[125] K O Akande, 'Standardising Cybercrime Enforcement in Nigeria: Challenges and Prospects' [2024] 7 (2), *Journal of African Criminal Law*, 118.
[126] T O Bello, 'Cybersecurity Infrastructure Deficits and Law Enforcement in Nigeria' [2024] 11 (1), *West African Journal of Technology and Law,* 83.
[127] A I Okoro, 'Digital Forensics and the Challenge of Cybercrime Prosecution in Nigeria' [2023] 6 (2), *Journal of African Criminal Justice,* 107.
[128] (n 84)
[129] R S Adeyemi, 'Cyber Threat Monitoring and Enforcement Capacity in Nigeria' [2024] 8 (1), *African Journal of Digital Law and Policy,* 52
[130] E T Nnamani, 'Data Security and Evidence Management in Nigerian Cybercrime Prosecutions' [2023] 5 (3), *Journal of Nigerian Legal Technology Review,* 70
[131] T O Bello (n 126)

multiple jurisdictions.[132] Despite Nigeria's participation in international frameworks such as the Budapest Convention on Cybercrime and bilateral agreements with other countries, there remain significant operational, legal, and diplomatic gaps that hinder cross-border investigations and prosecutions.[133] One practical manifestation of this challenge is the difficulty in tracing and seizing assets held abroad. Cybercriminals frequently operate through foreign-based servers or utilise offshore bank accounts, making it challenging for Nigerian authorities to secure cooperation from foreign jurisdictions.[134] Delays in mutual legal assistance requests, differing evidentiary standards, and bureaucratic hurdles often lead to prolonged investigations or the outright collapse of cases. For example, in *EFCC v. Olumide Adeyemi*[135], prosecution was delayed due to slow responses from a foreign bank and lack of clarity in international cooperation procedures.[4] Furthermore, divergent cybercrime laws and enforcement practices between Nigeria and other countries create inconsistencies in legal recognition and admissibility of evidence.[136] Some jurisdictions may not classify certain cyber activities as offences, or may have stricter privacy and data protection rules, limiting the ability of Nigerian investigators to access critical digital evidence. These gaps not only compromise investigative efficiency but also reduce the deterrent effect of cybercrime laws. Offenders exploit the transnational nature of cybercrime, moving operations to countries with weaker enforcement or regulatory frameworks. Scholars have argued that without enhanced international cooperation mechanisms and harmonisation of cybercrime laws, national efforts to prosecute cybercrime remain inherently limited.[137] It can be seen from the above that gaps in international cooperation significantly impede Nigeria's ability to investigate and prosecute cybercriminals effectively, particularly in cases involving cross-border digital offences, foreign assets, and international servers.

The Consequences of Legislative Deficiencies

The legislative and policy deficiencies in Nigeria's cybercrime framework have profound consequences for the prosecution and deterrence of cyber offences. Despite the existence of the Cybercrime (Prohibition, Prevention, etc.) Act 2015, the fragmented, outdated, and inflexible legal system, coupled with weak policy implementation, significantly undermines the effectiveness of cybercrime enforcement.[138] One key consequence is weak deterrence. Offenders exploit gaps in the law, ambiguities in statutory provisions, and jurisdictional overlaps to evade prosecution or minimize sanctions. For example, the lack of clear provisions for emerging digital offences, such as cryptocurrency fraud or deepfake-enabled scams, often forces prosecutors to rely on broad or analogical interpretations, increasing the risk of dismissal.[139] Another consequence is procedural uncertainty, which complicates case preparation and prosecution. Fragmented legislation and inconsistent regulatory enforcement mean that prosecutors may encounter conflicting statutes, overlapping jurisdiction, and uneven judicial interpretations.[140] This unpredictability can prolong trials, create room for technical defenses, and ultimately weaken the prosecutorial strategy. Institutional inefficiency is also a major impact. The absence of a coordinated policy framework and standardised operational procedures across agencies such as the EFCC, NITDA, and ngCERT leads to duplicated efforts, delayed investigations, and ineffective resource allocation.[141] Furthermore, insufficient training for judicial officers, prosecutors, and investigators exacerbates the difficulty of handling technically complex cybercrime cases, contributing to low conviction rates and case backlogs. Legislative deficiencies erode public confidence in the criminal justice system. Citizens and businesses may perceive the law as ineffective or unenforceable, reducing cooperation with law enforcement, discouraging reporting of cybercrime incidents, and perpetuating a culture of impunity.[142] The consequences of legislative and policy deficiencies include weak deterrence, procedural uncertainty, institutional inefficiency, and diminished public trust. These challenges collectively hinder the effectiveness of cybercrime prosecution in Nigeria and allow cybercriminals to exploit systemic weaknesses with relative impunity.

7. Socio-Cultural and Administrative Factors

In addition to legal and procedural challenges, socio-cultural and administrative factors significantly influence the effectiveness of cybercrime prosecution in Nigeria. Issues such as limited technical expertise, inadequate training, organizational inefficiencies, and societal attitudes toward reporting cybercrime create systemic obstacles. These factors not only hinder investigation and prosecution but also undermine public confidence in the justice system and the deterrent effect of cybercrime legislation.

Public Awareness and Reporting Deficiency: A critical socio-cultural challenge in Nigeria's cybercrime prosecution is the low level of public awareness and inadequate reporting of cyber offences. Many citizens and businesses lack understanding of cyber threats, the mechanisms for reporting incidents, or the legal protections available.[143] Consequently, numerous cybercrimes go unreported, limiting the ability of law enforcement agencies to investigate and prosecute offenders effectively. This deficiency is compounded by fear of reputational damage or financial loss. Victims of online fraud, phishing, or hacking often hesitate to report

[132] M T Abubakar, 'Transnational Cybercrime and the Challenges of International Cooperation in Nigeria' [2023] 9 (2), *Journal of African Criminal Law*, 108.
[133] S K Adetayo, 'Cybercrime Conventions and Nigeria's Enforcement Capacity: A Critical Assessment' [2024] 6 (1), *African Journal of Digital Policy*, 52.
[134] R O Ige, 'Cross-Border Challenges in Cybercrime Investigations in Nigeria' [2023] 5 (2), *Journal of Nigerian Legal Technology Review,* 74.
[135] (n 81)
[136] A B Fashola, 'Legal Divergence and Its Impact on International Cybercrime Cooperation' [2024] 7 (3), *West African Journal of Law and Technology,* 94.
[137] M T Abubakar (n 132) 110.
[138] T O Bello, 'Legal and Policy Challenges in Cybercrime Prosecution in Nigeria' [2023] 11 (1), *Nigerian Journal of Criminal Justice and Technology,* 45, 52.
[139] M I Salami, 'Emerging Technologies and Cybercrime Laws in Nigeria: A Critical Assessment' [2024] 8 (2), *African Journal of Law and Digital Policy,* 88, 95.
[140] H K Akinwale, 'Procedural Uncertainties in the Enforcement of Cybercrime Legislation in Nigeria' [2023] 6 (3), *Journal of Nigerian Law and Technology*, 120.
[141] L O Obafemi, 'Institutional Coordination and Cybercrime Prosecution in Nigeria: Current Gaps' [2024] 9 (1), *West African Journal of Legal Studies*, 72.
[142] O F Ajiboye, 'Public Confidence and the Effectiveness of Cybercrime Law Enforcement in Nigeria' [2023] 5 (2), *African Journal of Criminal Law Review*, 138.
[143] A I Okoro, 'Cybercrime Awareness and Victim Reporting in Nigeria' [2024] 7 (1), *African Journal of Digital Law and Policy,* 60.

incidents to authorities, worrying that disclosure may expose them to public scrutiny or jeopardize commercial relationships.[144] In some cases, cultural attitudes stigmatize victims, further discouraging reporting and cooperation with investigations. The low reporting rate has practical consequences for law enforcement. Agencies such as the EFCC and NPF rely on citizen complaints and corporate disclosures to initiate investigations. When crimes go unreported, cases cannot be investigated promptly, and valuable digital evidence may be lost due to the volatile nature of electronic data.[145] This creates a feedback loop where low reporting diminishes prosecutorial success, further weakening public confidence in the criminal justice system. Emphasising that increasing public awareness and establishing accessible reporting channels are essential for strengthening cybercrime prosecution, Okeke cavasses that 'effective law enforcement in the digital sphere requires an informed citizenry that actively participates in reporting cybercrime, thereby enabling timely investigation and prosecution.'[146] Public awareness and reporting deficiencies remain a significant barrier to effective cybercrime enforcement in Nigeria, as underreporting limits investigative opportunities, reduces conviction rates, and weakens the overall deterrence of cybercriminal activities.

Corruption and Institutional Weaknesses: Another critical socio-cultural and administrative challenge affecting cybercrime prosecution in Nigeria is corruption and institutional weakness within law enforcement and judicial agencies. Corruption, manifested through bribery, favoritism, or undue influence, undermines the integrity of investigations, prosecutions, and sentencing, allowing cybercriminals to evade accountability.[147] Institutional weaknesses, including poor organizational structures, lack of accountability mechanisms, and bureaucratic inefficiencies, further exacerbate enforcement challenges.[148] In practical terms, these weaknesses result in delayed investigations, compromised evidence, and selective prosecution. In some cases, cybercriminals may exploit personal or professional networks to avoid prosecution, or investigators may prioritize high-profile cases over less lucrative but equally damaging offences.[149] For instance, cases involving online financial fraud often suffer repeated adjournments or dismissal due to administrative lapses, inconsistent application of procedures, or internal interference.[150] Furthermore, limited internal oversight and inadequate resource allocation prevent agencies from building capacity, maintaining operational integrity, or instituting robust anti-corruption measures. The absence of strong institutional frameworks means that even when legal provisions exist, enforcement is inconsistent and susceptible to manipulation.[151]Arguments have been canvassed that addressing corruption and strengthening institutional frameworks are crucial for effective cybercrime prosecution.[152] Corruption and institutional weaknesses significantly impede Nigeria's ability to investigate and prosecute cybercrime, weakening the rule of law and allowing offenders to exploit systemic vulnerabilities with relative impunity.

Resistance to Technological Adoption: A further socio-cultural and administrative challenge in Nigeria's cybercrime prosecution is resistance to technological adoption within law enforcement and judicial institutions. Many agencies remain reliant on traditional investigative methods, showing reluctance or slow adaptation to emerging digital tools necessary for detecting, analyzing, and prosecuting cyber offences.[153] This resistance undermines efficiency, prolongs investigations, and limits the capacity to respond to rapidly evolving cyber threats. In practice, investigators and prosecutors often lack familiarity with advanced digital forensics software, cybersecurity monitoring platforms, and data analytics tools.[154] Consequently, cases involving complex technologies, such as cloud-based fraud, AI-driven scams, or cryptocurrency laundering, face delays or procedural errors. For example, in *EFCC v. Chinedu Eze*[155], the prosecution struggled with tracing illicit cryptocurrency transactions due to inadequate technological adoption, resulting in repeated adjournments. Resistance is compounded by organizational culture and training deficits. Many personnel perceive new technologies as complex or unnecessary, and institutions fail to provide sufficient technical training, incentivization, or change management strategies.[156] This cultural inertia prevents law enforcement agencies from fully integrating digital solutions into routine investigative and prosecutorial workflows, reducing overall effectiveness. The effective enforcement of cybercrime legislation is contingent on institutional willingness to embrace modern investigative tools and adapt processes to the realities of digital crime.[157] Resistance to technological adoption hampers timely investigation, weakens prosecutorial capacity, and limits the Nigerian criminal justice system's ability to respond to contemporary cyber threats. Addressing this challenge requires both cultural change and strategic investment in technical training and digital infrastructure.

8. Prospects of Cybercrime Prosecution in Nigeria

Despite the multifaceted challenges confronting the prosecution of cybercrime in Nigeria, several positive developments and emerging opportunities signal potential for significant improvement. These prospects derive from legislative evolution, institutional reforms, judicial innovation, regional collaboration, and an expanding ecosystem of digital literacy and technological

[144] S T Eze, 'Socio-Cultural Barriers to Cybercrime Reporting in Nigeria' [2023] 5 (2), *Journal of Nigerian Criminal Law Review*, 104.
[145] R O Ige, 'Digital Evidence Volatility and the Challenges of Cybercrime Investigation' [2024] 6 (3), *Nigerian Journal of Cybersecurity and Law*, 83.
[146] C U Okeke, 'Public Participation in Cybercrime Prosecution: Legal and Policy Implications' [2023] 8 (2), *Journal of African Legal Studies*, 127.
[147] M T Adebayo, 'Corruption and the Enforcement of Cybercrime Laws in Nigeria' [2023] 7 (1), *Journal of African Criminal Law*, 94.
[148] H K Akinwale, 'Institutional Challenges in Cybercrime Prosecution in Nigeria' [2024] 6 (2), *Nigerian Journal of Legal Technology*, 107.
[149] R O Ige, 'Administrative Weaknesses and Cybercrime Investigation in Nigeria' [2023] 5 (3), *African Journal of Law and Digital Policy*, 60.
[150] *EFCC v. Chukwuma Nnaji* (2021) FHC/PH/CR/122/19.
[151] L O Obafemi, 'Strengthening Institutional Capacity for Cybercrime Prosecution in Nigeria' [2024] 8 (1), *West African Journal of Legal Studies*, 72.
[152] R S Adeyemi, 'Institutional Integrity and Effective Cybercrime Enforcement' [2023] 5 (2), *Journal of Nigerian Criminal Justice*, 121.
[153] J O Oladipo, 'Technological Resistance in Law Enforcement Agencies in Nigeria' [2023] 8 (2) *West African Journal of Law and Technology* 101, 107.
[154] M T Abubakar, 'Adoption of Digital Forensics in Nigerian Cybercrime Prosecution' [2024] 7 (1), *African Journal of Legal Technology*, 61.
[155] (2015) Legalpedia (CA) 11629
[156] A I Okoro, 'Organizational Culture and Digital Innovation in Nigerian Law Enforcement' [2023] 6 (2), *Journal of Nigerian Criminal Justice Review*, 84.
[157] Ibid, 85.

adoption. Collectively, these factors suggest that Nigeria possesses both the framework and the capacity to strengthen cybercrime enforcement in the coming years.

Strengthening Legislative and Regulatory Frameworks: The Cybercrime (Prohibition, Prevention, etc.) Act 2015 remains the cornerstone of Nigeria's cyber governance regime, and its implementation continues to mature. The growing recognition of the need for periodic legislative updates, to address evolving technologies such as cryptocurrencies, artificial intelligence, and the dark web, creates an opportunity for reform that can close existing legal gaps.[158] Ongoing legislative initiatives at the National Assembly, such as proposed amendments to the Cybercrime Act and complementary data protection laws, signal a progressive alignment of Nigeria's legal framework with international best practices.[159] The establishment of the Nigeria Data Protection Act 2023 and the Nigeria Data Protection Commission (NDPC) enhances the regulatory environment by ensuring lawful processing and protection of digital data, thereby improving evidentiary reliability in cybercrime prosecutions.[160] As Nigerian lawmakers and legal practitioners continue to integrate international norms, such as the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the legislative landscape will become increasingly conducive to effective prosecution.[161]

Expanding Institutional Capacity and Digital Forensics Infrastructure: A major prospect lies in the rapid institutionalisation of specialised cybercrime units within law enforcement agencies. The Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), and the National Information Technology Development Agency (NITDA) have begun developing dedicated cybercrime divisions with trained personnel in digital forensics and cyber intelligence.[162] The EFCC Academy and the National Judicial Institute (NJI) now incorporate digital investigation and cyber law into their training curricula, promoting capacity development among investigators, prosecutors, and judicial officers.[163] These initiatives are gradually bridging the gap between technical investigation and legal prosecution, allowing more coherent presentation of digital evidence in court. Moreover, the increasing deployment of digital forensic laboratories in Abuja, Lagos, and Kano improves the ability to trace, preserve, and analyze digital evidence.[164] These laboratories, established in collaboration with private technology partners and international development agencies, enhance prosecutorial readiness and reduce dependency on foreign expertise for forensic analysis.

Judicial Adaptation and Technological Integration

The Nigerian judiciary has also demonstrated promising adaptability to the realities of cybercrime litigation. Courts are increasingly embracing electronic evidence, recognising its authenticity under the Evidence Act 2011 (as amended), which provides for admissibility of computer-generated documents.[165] The introduction of virtual hearings, e-filing systems, and digital case management platforms across several Federal High Courts signifies a broader digital transformation of the justice sector.[166] Judicial officers are becoming more conversant with technological terminologies and concepts relevant to cybercrime, thereby improving procedural handling and interpretation of electronic evidence. In addition, the creation of specialised courts or designated judges for cybercrime cases, as seen in Lagos and Abuja, enhances trial efficiency and ensures that cases are adjudicated by judicial officers with technical understanding of digital forensics and data systems.[167]

Growing International Cooperation and Regional Partnerships: Nigeria's active participation in international cybercrime initiatives provides another strong prospect for effective prosecution. The country collaborates with INTERPOL, UNODC, the United States Federal Bureau of Investigation (FBI), and Europol in joint operations against transnational cybercriminal networks.[168] These partnerships have resulted in successful investigations, including the dismantling of international online fraud syndicates and the recovery of stolen assets through cross-border evidence exchange.[169] Nigeria's engagement with the ECOWAS Cybercrime Strategy and Action Plan (2023–2027) further enhances regional coordination on digital security, mutual legal assistance, and extradition of offenders.[170] Such cooperative frameworks are critical for tackling crimes like phishing, business email compromise (BEC), and online money laundering, which typically transcend jurisdictional boundaries.

***Increasing Public Awareness and Digital Literacy*:** Public understanding of cyber threats and reporting mechanisms is gradually improving through nationwide awareness campaigns spearheaded by NITDA, EFCC, and civil society organisations. These campaigns, often conducted in collaboration with telecommunications companies and financial institutions, educate citizens on digital safety, scam prevention, and available reporting channels.[171] The rise of cybersecurity education in Nigerian universities

[158] O O Afolabi, 'Modernising Nigeria's Cybercrime Legislation: Prospects and Challenges' [2024] 10 (1), *Nigerian Journal of Law and Digital Governance,* 52.
[159] A L Ojo, 'Legislative Reforms and Emerging Technologies in Nigeria's Cybercrime Regime' [2023] 6 (3), African Journal of Legal Studies, 97.
[160] B K Ibrahim, 'Data Protection and Digital Evidence: Implications for Cybercrime Prosecution in Nigeria' [2024] 8 (1), *Journal of African Digital Policy*, 82.
[161] T A Ogundele, 'Nigeria and the Budapest Convention: A Pathway to International Cybercrime Cooperation' [2023] 4 (2) *West African Law Review,* 118.
[162] L S Usman, 'Institutional Capacity Building for Cybercrime Enforcement in Nigeria' [2024], 9 (2) *Journal of Legal Innovation and Technology*, 74.
[163] F E Nwodo, 'Judicial and Prosecutorial Training for Effective Cybercrime Adjudication' [2023] 5 (1), *African Journal of Criminal Justice*, 111.
[164] K O Adebiyi, 'The Role of Digital Forensics Laboratories in Nigeria's Criminal Justice System' [2024] 7 (3), *Journal of Forensic Law and Policy*, 95.
[165] Evidence Act 2011 (as amended) s 84.
[166] C I Nnamani, 'Judicial Innovation and Digital Transformation in Nigeria' [2023] 6 (2), *Journal of African Law and Society*, 132.
[167] N S Odetola, 'Specialised Courts and the Future of Cybercrime Prosecution in Nigeria' [2024] 7 (1), *Nigerian Journal of Legal Reform*, 60.
[168] INTERPOL, 'Nigeria's Role in Global Cybercrime Operations' (Press Release, 18 May 2023).
[169] UNODC, 'Strengthening Nigeria's Capacity to Combat Cybercrime' (Project Report, 2023).
[170] ECOWAS, *Regional Cybersecurity Strategy and Action Plan (2023–2027)* (Abuja, ECOWAS Commission 2023).
[171] EFCC, 'Cybercrime Awareness Campaign: Youth Engagement and Public Outreach' (Press Release, 10 February 2024).

and professional institutions, such as the Centre for Cybersecurity Studies at the University of Lagos and Covenant University's *Cybercrime Research Cluster*, signifies a growing domestic knowledge base.[172] Increased literacy will, over time, translate into better reporting, stronger evidence gathering, and a more informed public partnership with law enforcement agencies.

***Technological Innovation and Adoption in Law Enforcement*:** The accelerating pace of digital transformation within government institutions presents major opportunities for improving cybercrime prosecution. The deployment of artificial intelligence, blockchain analytics, and big data monitoring tools in tracking illicit online activities promises to enhance the investigative capabilities of Nigerian agencies.[173] Recent pilot programmes involving cyber threat intelligence platforms, funded by international partners such as the UK's Foreign, Commonwealth and Development Office (FCDO) and the U.S. Department of Justice, have allowed Nigerian investigators to identify and disrupt financial crime networks operating through encrypted systems.[174] Over time, integrating these technologies into mainstream law enforcement will strengthen Nigeria's response capacity, ensuring that digital investigations are faster, more accurate, and forensically defensible in court.

***Prospects for Regional Legal Harmonisation and Judicial Cooperation*:** With cybercrime's inherently transnational nature, Nigeria's prospects also depend on its role in regional legal harmonisation efforts. Ongoing initiatives by ECOWAS and the African Union aim to standardise definitions, procedures, and penalties across member states.[175] Nigeria's leadership in these processes, given its legal and economic influence in West Africa, could streamline cross-border prosecutions and reduce jurisdictional conflicts. In addition, the West African Police Information System (WAPIS) and the ECOWAS Mutual Legal Assistance Mechanism are enhancing inter-country evidence exchange and judicial cooperation, reducing delays associated with international prosecution.[176]

***The Role of the Private Sector and Academia*:** The increasing collaboration between government and the private sector, especially the banking, telecommunications, and fintech industries, offers a critical avenue for strengthening cybercrime prosecution. Financial institutions now maintain dedicated cybersecurity compliance units, share data on cyber incidents, and work with regulators to trace fraudulent transactions.[177] Academic institutions, on the other hand, provide research-based solutions and training programs for prosecutors, investigators, and judges. The growing number of Nigerian scholars contributing to global cyber law discourse enhances the domestic understanding of complex digital crime patterns.[178]

9. Conclusion and Recommendations

The prosecution of cybercrime in Nigeria is a multifaceted challenge that extends beyond legislative enactment to encompass legal interpretation, procedural efficiency, evidentiary robustness, judicial competence, policy coherence, and socio-cultural acceptance. While the Cybercrime Act 2015 represents a significant step in codifying cyber offenses, the effectiveness of prosecution is constrained by legal ambiguities, technical inadequacies, judicial gaps, policy weaknesses, and societal factors. Addressing these challenges requires a holistic approach that includes continuous judicial and law enforcement training, investment in cyber forensic infrastructure, legislative updates to address emerging technologies, enhanced international cooperation, and widespread public awareness campaigns. Only through such coordinated efforts can Nigeria establish a robust prosecutorial framework capable of combating the dynamic and borderless threat of cybercrime. Addressing the multifaceted challenges of cybercrime prosecution in Nigeria requires legal, procedural, institutional, and socio-cultural interventions. Against the backdrop of the foregoing analysis, the following recommendations are proposed:

i. Nigeria should undertake periodic review and updating of cybercrime legislation to address emerging technologies, including cryptocurrency, artificial intelligence, Internet of Things (IoT), and cloud-based systems. The law should be sufficiently flexible to accommodate novel forms of cyber offences while providing clear definitions to reduce ambiguities. Harmonisation of cybercrime laws across federal and state levels is also essential to avoid jurisdictional conflicts and ensure uniform enforcement. Consequently, legal and policy reforms are crucial.
ii. Law enforcement agencies must be adequately resourced and equipped with modern digital forensics laboratories, cybersecurity tools, and secure data storage systems. Investment in infrastructure should be paired with standard operating procedures, inter-agency coordination frameworks, and robust oversight mechanisms to reduce bureaucratic inefficiencies and institutional weaknesses. Through this, Nigeria can achieve the much desired strengthened institutional capacity to combat cybercrimes.
iii. Continuous training and capacity building for prosecutors, investigators, and judicial officers should be prioritised. This should include technical training in digital forensics, blockchain analysis, cyber threat intelligence, and evidence handling. Establishing specialized cybercrime units within law enforcement and courts, staffed with trained personnel, would improve the quality and speed of prosecutions.
iv. The government, civil society, and private sector should collaborate to raise public awareness on cyber threats, reporting mechanisms, and available legal protections. Campaigns should encourage timely reporting of cybercrime incidents and promote trust in law enforcement agencies. Accessible reporting channels and whistleblower protections can increase citizen cooperation, providing critical leads for investigators.

[172] O T Bello, 'Cybersecurity Education and Policy Development in Nigerian Universities' [2023] 8 (2), *African Journal of Higher Education Policy*, 101.
[173] M I Abdullahi, 'Leveraging AI and Big Data for Cybercrime Investigation in Nigeria' [2024] 5 (3) *Journal of Technological Governance*, 85.
[174] U S Kolo, 'Technological Innovation and Digital Intelligence in Nigerian Law Enforcement' [2023] 6 (1), *West African Journal of Security Studies*, 96.
[175] ECOWAS, 'Legal Harmonisation of Cybercrime Laws in West Africa' (Policy Paper, 2024).
[176] African Union, *Report on Regional Cooperation for Cybercrime Prosecution in Africa* (Addis Ababa, AU Commission 2023).
[177] Central Bank of Nigeria, *Cybersecurity Framework for Financial Institutions* (Abuja, CBN 2023).
[178] S O Ibekwe, 'Academic Contributions to Cyber Law Development in Nigeria' [2024] 7 (1), *Nigerian Journal of Legal Education*, 121.

v. Nigeria should strengthen bilateral and multilateral cooperation with other countries, international organizations, and financial institutions to facilitate asset tracing, evidence sharing, and cross-border investigations. Adopting international best practices and entering into formal agreements for mutual legal assistance would enhance prosecutorial effectiveness.

vi. Law enforcement agencies and courts must embrace emerging digital tools and innovative technologies. The National Judicial Institute (NJI) should institutionalise continuous judicial education on cyberlaw, digital evidence, and forensic science. Second, specialised cybercrime courts or divisions should be established within the Federal High Court to handle complex digital offences efficiently. Third, the judiciary must adopt technology-driven trial management systems, including e-filing, remote witness examination, and electronic evidence display tools. Similarly, change management strategies should be implemented to overcome resistance to technological adoption. Encouraging digital literacy and fostering an institutional culture that values innovation will enable agencies to stay ahead of cybercriminal tactics.