ELECTRONIC EVIDENCE IN CYBERCRIME PROSECUTIONS IN NIGERIA: AN APPRAISAL OF THE LEGAL FRAMEWORK, JUDICIAL APPROACHES AND EMERGING CHALLENGES

Abstract
The rapid digitization of criminal activities has made electronic evidence central to the administration of criminal justice in Nigeria. With the enactment of the Evidence Act 2011 (as amended in 2023) and the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, the Nigerian legislature sought to establish clear pathways for the admissibility and utilization of digital proof. However, the practical application of these statutory regimes in cybercrime prosecutions reveals systemic hurdles. Prosecutors frequently encounter barriers relating to the strict interpretation of certification requirements, fragile forensic custody chains, technological deficits within law enforcement agencies, and the complexities of cross-border data retrieval. This article conducts a critical appraisal of this legal framework, examining the statutory provisions of Section 84 of the Evidence Act 2011 alongside evolving judicial interpretations. Employing a doctrinal methodology, the paper analyzes the judicial insistence on strict compliance with certification protocols and contrasts local challenges with developments in India and the European Union. The paper finds that the current framework is overly rigid in its certification demands and structurally unequipped for cloud-based and decentralized digital environments. It recommends legislative amendments to Section 84 to accommodate third-party digital custodians, the institutionalization of standard forensic operational procedures, and the fast-tracking of international mutual legal assistance treaties.

Keywords: Electronic Evidence, Cybercrime, Section 84, Admissibility, Digital Forensics, Nigeria.

1. Introduction

The transition from paper-based transactions to digital systems has transformed the landscape of criminal investigations. Traditional offences, such as obtaining by false pretences and forgery, are now routinely executed through electronic communication systems, while sophisticated digital threats including ransomware, business email compromise (BEC), and unauthorized system intrusion, have grown more prevalent. Because these modern infractions occur within virtual spaces, physical traces are increasingly rare. Consequently, the prosecution of cybercrimes depends almost exclusively on electronic evidence, ranging from system logs, IP addresses, and database entries to email correspondence, social media interactions, and instant messaging transcripts.

Unlike physical items of proof, electronic data is inherently volatile, easily manipulated, and capable of being modified, deleted, or fabricated without leaving readily apparent physical evidence. Moreover, digital information is frequently stored across distributed systems, cloud servers, or third-party platforms located in foreign jurisdictions. These characteristics present a significant challenge to traditional rules of evidence, which were historically designed for tangible documentary and real evidence.

Nigeria attempted to address these challenges by replacing the old 1990 Evidence Act with the Evidence Act 2011 (subsequently amended in 2023), which introduced specific provisions governing the admissibility of computer-generated documents and cloud-based electronic records. This was augmented by the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, which criminalizes various computer-related activities, revises provisions on offensive online communications, and establishes refined mechanisms for electronic data preservation.

Despite these legislative developments, the prosecution of cybercrime in Nigeria remains constrained by systemic legal, institutional, and operational challenges. Trial courts often struggle to balance the need for authenticating digital evidence under Section 84 of the Evidence Act with the practical realities of digital forensics. Furthermore, investigative agencies frequently operate under severe technical and infrastructural constraints, occasionally compromising the integrity of the chain of custody before evidence reaches the courtroom.

This article conducts a comprehensive evaluation of the legal and institutional framework regulating electronic evidence in Nigerian cybercrime prosecutions. It analyzes the statutory requirements, maps out the institutional

***Ngozi Chisom Uzoka, LLB, BL, LLM, PhD**, Reader, Department of Private & Property Law, Faculty of Law, Nnamdi Azikiwe University Awka, Nigeria. Email: nc.uzoka@unizik.edu.ng
****Ifeoma C. Nnadozie Oguejiofor**, **LLB, BL,** LLM Candidate**,** Faculty of Law, Nnamdi Azikiwe University Awka, Nigeria; State Counsel, Ministry of Justice, Anambra State, Nigeria.

enforcement mechanisms, traces the evolution of judicial approaches, identifies systemic challenges, and offers comparative insights to suggest practical legislative and structural reforms.

2. The Legal and Regulatory Framework for Electronic Evidence in Nigeria

A. The 1999 Constitution of the Federal Republic of Nigeria (As amended)

The collection and presentation of electronic evidence do not occur in a vacuum; they are bound by the constitutional protections enshrined in the Constitution of the Federal Republic of Nigeria 1999 (as amended).[1] Specifically, Section 37 guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications.[2]

In cybercrime investigations, this right frequently conflicts with the state's interest in intercepting communications, searching digital devices, and seizing electronic data. While investigative agencies enjoy broad search and seizure powers under various penal statutes, any electronic evidence obtained in flagrant violation of Section 37 risks exclusion. Under Section 357 of the Administration of Criminal Justice Act (ACJA) 2015,[3] and emerging judicial trends, courts must balance the probative value of illegally or improperly obtained evidence against the public interest and the severity of the constitutional infringement.

B. Section 84 of the Evidence Act 2011: The Admissibility Threshold

The primary statutory mechanism for the reception of digital proof in Nigerian courts is Section 84 of the Evidence Act 2011.[4] Section 84(1) provides that in any proceedings, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, provided the conditions in Section 84(2) are satisfied. These conditions require the proponent of the evidence to establish that:

1. The computer was regularly used to store or process information for the purposes of any activities regularly carried on over that period;[5]
2. Supply of the information to the computer was regularly done in the ordinary course of those activities;[6]
3. Throughout the material part of that period, the computer was operating properly or, if not, that any respect in which it was not operating properly was not such as to affect the production of the document or the accuracy of its contents;[7] and
4. The information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of activities.[8]

To substantiate these technical conditions, Section 84(4) mandates the presentation of a certificate signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities.[9]The certificate must identify the document containing the statement, describe the manner in which it was produced, and give particulars of the device used.

The procedural pathway established under Section 84 operates as a strict multi-tiered filter for the courts. At the initial stage, the court determines the legal character of the tendered proof. If the item is classified as noncomputer-generated, the standard common-law rules of documentary evidence apply. However, if the evidence is computer-generated, it must undergo a secondary level of evaluation to satisfy the conditions of Section 84(2) regarding the operational status of the computer during the material period.

The final hurdle requires the production of a valid certificate of authentication under Section 84(4). Where the presenting party fails to supply this certificate, the electronic document is deemed legally incompetent and inadmissible, in line with the landmark ruling in *Kubor v. Dickson*.[10] Conversely, when a proper certificate is provided, the evidence crosses the threshold of admissibility, allowing the court to progress to a technical audit of the document's contents, metadata, and overall probative weight.

---

[1] Constitution of the Federal Republic of Nigeria 1999 (as amended).
[2] Constitution of the Federal Republic of Nigeria 1999, s 37.
[3] Administration of Criminal Justice Act 2015, Act No. 3, s 357.
[4] Evidence Act 2011, s 84(1).
[5] Evidence Act 2011, s 84(2)(a).
[6] Evidence Act 2011, s 84(2)(b).
[7] Evidence Act 2011, s 84(2)(c).
[8] Evidence Act 2011, s 84(2)(d).
[9] Evidence Act 2011, s 84(4).
[10] *Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534 (SC).

This statutory architecture shifts the focus of authentication from the contents of the document to the functional integrity of the computer system that generated it. While designed to prevent the introduction of fabricated or corrupted data, the practical enforcement of this provision has created a demanding procedural hurdle in criminal trials, especially where the prosecuting agency does not own or control the computer system that recorded the evidence.

This statutory architecture underwent a significant transformation with the enactment of the Evidence (Amendment) Act 2023[11]. Recognizing that the principal 2011 Act lagged behind global technological shifts, the 2023 legislature expanded the wording of Section 84(2) and (4) to explicitly include 'electronic records' alongside computer-generated documents. More crucially, the amendment introduced novel provisions under Sections 84A, 84B, 84C, and 84D. Section 84B explicitly provides that information stored, recorded, or copied in cloud computing environments, optical or magnetic media, or decentralized databases produced by a computer shall be treated as directly admissible documents without requiring strict proof of the physical original. Furthermore, Section 84C gives formal statutory recognition to digital signatures as a valid tool for authenticating electronic records. While these additions structurally modernize the text of the law, they simultaneously deepen the procedural complexities for trial prosecutors, who must now navigate the technical boundary between standard computer printouts and fluid, remote cloud databases.

C. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024

While the Evidence Act governs the admissibility of digital proof, the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 provides the substantive and procedural framework for investigating and prosecuting digital offenses. The 2024 Amendment brought critical legislative updates to the principal 2015 framework, notably restructuring Section 24 to remedy previous constitutional ambiguities regarding cyberstalking and freedom of expression. The Act empowers law enforcement officers to search cell phones, computers, and external storage media, and to compel service providers to assist in the preservation of electronic communication.

Section 38 of the Act imposes an obligation on mobile networks and internet service providers to retain traffic data and subscriber information for a minimum of two years.[12] This data is invaluable for establishing the identity of cyber-offenders through IP address allocation and cell tower routing. However, the Act contains procedural gaps regarding the precise forensic protocols that officers must observe during the seizure and extraction of this data, leaving the integrity of the collected information highly dependent on the subjective practices of individual investigators.

D. Procedural Laws: ACJA 2015 and State Equivalents

The ACJA 2015 attempts to modernize criminal trials by incorporating technological advancements into procedural administration. Section 15(4) of the ACJA allows the recording of a suspect's confessional statement on video, or its reduction to writing in the presence of the suspect's legal practitioner.[13] This provision is designed to mitigate trial-within-trial disputes regarding the voluntariness of confessions.

Where the prosecution relies on an electronic recording of a confession, it must satisfy the requirements of Section 84 of the Evidence Act 2011. While this procedural integration improves transparency, it demands a level of technical compliance that many police commands across Nigeria struggle to maintain due to poor infrastructural support.

3. The Institutional Framework for Cybercrime Prosecution and Electronic Evidence Management

Understanding the challenges of electronic evidence requires a critical examination of these institutional bodies, their mandates, and the practical frictions that emerge during inter-agency collaboration and evidence custody.

A. The Office of the National Security Adviser (ONSA)

Under Section 41 of the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, ONSA is designated as the coordinating hub for cybersecurity policies and strategies in Nigeria. ONSA oversees the National Cyber Security Advisory Council and manages the Nigeria Computer Emergency Response Team (ngCERT). The institutional mandate of ONSA is strategic rather than prosecutorial, focusing primarily on the protection of Critical National Information Infrastructure (CNII), such as banking telecommunication networks,

[11] Evidence (Amendment) Act 2023, ss 2 & 3.
[12] Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, s 38.
[13] Administration of Criminal Justice Act 2015, s 15(4).

national identity databases, and power grids. However, because ONSA serves as the central clearinghouse for cross-border cyber threat intelligence, a disconnect often

exists between the high-level digital intelligence ingested by ngCERT and the frontline investigative capacity of state police commands. Prosecutors frequently find that intelligence generated at the ONSA level requires significant restructuring to fit the strict evidentiary templates mandated by Section 84 of the Evidence Act when presented in open court.

B. The Nigeria Police Force National Cybercrime Centre (NPF-NCCC)

The frontline law enforcement agency tasked with investigating digital offenses is the Nigeria Police Force, which has centralized its technical capabilities under the National Cybercrime Centre (NPF-NCCC). Headquartered in Abuja and operating specialized digital intelligence wings across various zonal commands, the NPF-NCCC deployment includes dedicated incident reporting platforms, cyber-intelligence monitoring, and device extraction labs. The NPF-NCCC serves as the primary collector of digital devices, network logs, and hardware that ultimately form the baseline of computer-generated evidence. The operational reality, however, is characterized by a deep disparity between the centralized expertise within the NPF-NCCC headquarters and the peripheral capabilities of divisions and stations in interior jurisdictions. In thousands of local police formations across Nigeria, routine criminal cases involving digital components, such as WhatsApp threats, mobile banking fraud, or email spoofing are handled by general duties officers who lack basic digital hygiene training. Devices are frequently handled without write-blockers, SIM cards are left active inside seized phones (allowing remote wiping), and certificates under Section 84(4) are either omitted entirely or poorly drafted by non-technical investigators, resulting in routine dismissals at trial.

C. The Economic and Financial Crimes Commission (EFCC)

The EFCC holds a robust enforcement footprint in the cybercrime space, particularly regarding advance fee fraud, internet scams, and business email compromise (BEC). Backed by a specialized Cybercrime Section and a Directorate of Forensic Science, the EFCC has institutionalized a highly technical workflow for extracting and documenting electronic evidence. The commission routinely utilizes specialized software tools to preserve digital chains of custody and systematically structures its forensic reports to accompany the statutory certificates required by Section 84. Despite these institutional advances, the EFCC faces unique structural hurdles regarding institutional overreach and jurisdiction. Because the commission's primary statutory focus is financial crime, digital offenses lacking a clear nexus to monetary fraud are frequently down-prioritized, creating an enforcement gap for non-economic cybercrimes such as cyberstalking, system sabotage, and data breaches. Additionally, the high volume of parallel investigations taxes the institutional capacity of its digital forensics laboratories, leading to significant backlogs that delay the timely presentation of certified electronic evidence in time-sensitive trials.

D. Inter-Agency Friction and the Lack of a Central Repository

A critical institutional vulnerability in Nigeria's cybercrime framework is the horizontal fragmentation of digital forensic capabilities. The NPF-NCCC, the EFCC, the Department of State Services (DSS), and the Nigeria Customs Service all operate independent, non-communicating digital forensic labs and databases. These institutional silos prevent the cross-referencing of digital intelligence. For instance, an IP address or cryptographic wallet address flagged by the EFCC in Lagos may not be visible to an NPF-NCCC investigator analyzing a parallel corporate intrusion case in Abuja or Onitsha. More importantly, Nigeria lacks a standardized, nationally accredited repository for digital evidence preservation. In the absence of a unified institutional protocol, each agency establishes its own metadata baselines and internal standards for fulfilling Section 84 requirements, leaving judges with the burdensome task of navigating wildly divergent technical reports and certification standards across different law enforcement agencies.

4. Evolution of Judicial Approaches to Section 84

A. The Formalist Era: Strict Compliance and Inadmissibility

Following the passage of the Evidence Act 2011, the Supreme Court of Nigeria adopted a strict, literal interpretation of Section 84. The locus *classicus* remains *Kubor v. Dickson*, where the Supreme Court held that internet printouts and computer-generated documents are inadmissible without the accompanying certificate required under Section 84(4). This strict stance was reinforced in *Dickson v. Sylva*,[14] where the court emphasized that compliance with the certification process is a condition precedent to admissibility and cannot be waived by parties.

[14] *Dickson v Sylva* (2017) 8 NWLR (Pt 1567) 167 (SC).

In criminal prosecutions, this formalist approach has occasionally resulted in the exclusion of reliable electronic proof. In cases where the prosecution tendered call detail records (CDRs) or bank account statements without the required certificate, appellate courts routinely set aside convictions, treating the absence of the certificate as a fatal procedural error rather than a curable defect.[15]

B. The Transition Toward Systemic Reliability

Recognizing that an overly rigid application of Section 84 can frustrate the ends of justice especially when dealing with dynamic and cloud-stored data, the judiciary has gradually moved toward a more functional approach. In *Omisore v. Aregbesola,* [16] the court noted that where a witness tenders a computer-generated document from a system, they personally operated, their oral testimony regarding the proper functioning of the computer could, in certain circumstances, satisfy the statutory requirements of Section 84(2), even in the absence of a formal, separate paper certificate.

Similarly, in *Federal Republic of Nigeria v. Idoko*,[17] the Court of Appeal clarified that while admissibility is governed by Section 84, the ultimate probative value of the evidence depends on a broader judicial evaluation of its reliability. The court indicated that the mere production of a certificate does not shield electronic evidence from a technical audit regarding its integrity, custody chain, and vulnerability to tampering. This shift reflects a growing judicial awareness that a paper certificate is not a guarantee of digital authenticity.

5. Systemic and Operational Challenges in Cybercrime Prosecutions in Nigeria.

A. The "Third-Party Custody" Dilemma

The most pressing doctrinal challenge under Section 84 occurs when the electronic evidence is located on a computer system owned or controlled by an uncooperative third party or a foreign entity. For example, in a BEC prosecution, the critical evidence may reside on the servers of international email service providers (such as Microsoft or Google) or within decentralized cloud databases.

Because the Nigerian prosecuting authority (such as the EFCC or NPF-NCCC) does not control these servers, it is practically impossible to obtain a Section 84(4) certificate signed by the system administrators of these multinational companies. Under a strict reading of *Kubor v. Dickson*, such evidence remains technically inadmissible. Unlike physical evidence, where secondary evidence can easily be introduced, the statutory hurdle of Section 84 leaves little room for flexibility when a certificate cannot be secured.

This structural impasse has drawn intense scrutiny from Nigerian legal scholars. Nweze[18] argues that Section 84 treats digital evidence with an unmerited level of suspicion, imposing an asymmetric burden on prosecutors who rely on records generated by independent, third-party technology conglomerates like Meta or Google. This perspective is reinforced by Ikpeze,[19] who contends that the Nigerian judiciary's strict application of the certification requirement creates a systematic enforcement deficit, effectively shielding sophisticated cybercriminals whose operational footprints are intentionally distributed across uncooperative corporate servers. Conversely, Atekha[20] adopts a more defensive posture, asserting that the rigid demand for a Section 84(4) certificate serves as an indispensable constitutional bulwark against state-sponsored evidence fabrication and digital manipulation by overzealous law enforcement units. However, as Olowonyo[24] observes, even with the passage of the Evidence (Amendment) Act 2023, the underlying dilemma remains unresolved. Olowonyo notes that while Section 84B legalizes the admissibility of cloud-based electronic records, it fails to alter the fundamental reality that an external certificate or expert verification is still structurally required to validate system functionality during trial. Consequently, the contemporary consensus among academic writers leans toward a structural compromise: the law must transition from a formalist preoccupation with paper certificates toward a dynamic framework focused on the scientific reliability of the data's cryptographic chain of custody.

[15] See Nwosu v Federal Republic of Nigeria (2016) LPELR-40014 (CA).
[16] *Omisore v Aregbesola* (2015) 15 NWLR (Pt 1482) 205 (SC).
[17] *Federal Republic of Nigeria v Idoko* (2021) LPELR-56677 (CA).
[18] CC Nweze, 'Digital Admissibility Hurdles in Sub-Saharan Africa' (2022) 14 *UNIZIK Law Journal* 88.
[19] VO Ikpeze, 'Cyber-Prosecutions and the Rigidity of Section 84' (2024) 5 *NAU Law Review* 112.
[20] JA Atekha, 'Constitutional Safeguards and Electronic Proof' (2023) 9 *Nigerian Journal of Evidence Law* 45.
[24] AA Olowonyo, 'The Evidence (Amendment) Act 2023: A Critical Appraisal of Cloud Data Admissibility' (2025) 11 *Journal of Digital Litigation* 19.

B. Fragile Forensic Chains of Custody

Digital evidence is highly volatile. The simple act of booting up a seized laptop can alter system metadata, such as "last accessed" timestamps, potentially compromising its integrity for trial. Maintaining a secure chain of custody requires investigators to:

1. Isolate the device from network connections (using Faraday bags) to prevent remote wiping;
2. Generate a bit-stream physical image of the storage media;
3. Verify the mathematical integrity of the copy using cryptographic hashing algorithms (e.g., MD5 or SHA256); and
4. Conduct all forensic analyses strictly on the duplicate image rather than the original drive.

In Nigeria, many police cybercrime units lack the specialized equipment, write-blockers, and certified forensic software (such as EnCase or FTK) necessary to perform these operations. Consequently, digital evidence is frequently extracted using unscientific methods, leaving it vulnerable to defence challenges during crossexamination.

C. Cross-Border Latency Gaps

Cybercriminals operating in Nigeria frequently utilize infrastructure hosted abroad to launch attacks or store stolen data. To retrieve this information, Nigerian authorities must rely on Mutual Legal Assistance Treaties (MLATs) or formal letters rogatory.

The practical retrieval of this cross-border data is severely hindered by a critical operational latency gap. The operational latency gap functions as a progressive degradation timeline for volatile digital evidence. At the immediate onset of a cyber incident, data exists in its most pristine state on foreign servers, representing the peak opportunity for law enforcement retrieval. However, during months one to three, as domestic prosecutors handle the administrative realities of drafting and routing formal Mutual Legal Assistance Treaty (MLAT) requests through complex diplomatic channels, the targeted data undergoes a high risk of automated server rotations and standard corporate retention wipes.

Between months four to eight, while the bureaucratic paperwork slowly winds its way through foreign sovereign departments, the suspect maintains a critical window of opportunity to execute remote data wipes or overwrite records entirely. Consequently, by month nine and beyond when a formal diplomatic response is finally processed and returned to Nigerian investigators the critical electronic data is almost entirely unrecoverable, overwritten, or structurally compromised. This long delay effectively undermines the viability of the prosecution before the evidence can ever reach a Nigerian courtroom

6. Comparative Jurisprudence: Lessons from India and the European Union

A. India: The Evolving Interpretation of Section 65B of the Evidence Act

Section 65B of the Indian Evidence Act 1872 is virtually identical to Section 84 of the Nigerian Evidence Act 2011. For years, Indian courts grappled with whether the certificate requirement was mandatory under all circumstances. In *Anvar P.V. v. P.K. Basheer*,[21] the Supreme Court of India ruled that oral evidence could not substitute for the written certificate under Section 65B(4).

However, recognizing the hardship this caused when dealing with third-party devices, the Indian Supreme Court revised this position in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*.[22] The court held that while the certificate remains mandatory as a general rule, a party cannot be compelled to perform the impossible (*lex non cogit ad impossibilia*). Where the required certificate cannot be obtained despite diligent efforts such as when the device is controlled by an uncooperative third party the court may dispense with the certificate and allow the party to prove the integrity of the electronic record through other reliable means, including expert testimony. This pragmatic exception is highly relevant for Nigerian courts struggling with the rigid application of Section 84.

B. The European Union: Cross-Border Data Retrieval and the EncroChat Precedent

The European Union has moved away from slow bilateral assistance treaties toward expedited regional mechanisms. The EU's "e-Evidence" regulation framework allows judicial authorities in one member state to issue direct European Production Orders to service providers located in another member state, bypassing diplomatic channels and reducing retrieval times to days or hours.

[21] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473 (SC).
[22] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* AIR 2020 SC 4908.

Furthermore, the European Court of Justice (CJEU) in the *EncroChat* case (*M.N.*)[23] examined the admissibility of encrypted telecommunications data intercepted across borders. The CJEU ruled that while member states enjoy latitude in gathering electronic intelligence, they must respect fundamental rights, maintaining robust procedural safeguards to ensure the intercepted data remains authentic and open to adversarial challenge by the defense. This jurisprudence emphasizes that technological efficiency in cybercrime investigations must not come at the expense of constitutional fair hearing standards.

7. Recommendations

To resolve these statutory, judicial, and operational bottlenecks, the following interventions are recommended:

A. Legislative Reform of Section 84

The National Assembly should amend Section 84 of the Evidence Act 2011 to introduce a statutory exception to the certification requirement. Mirroring India's *Arjun Panditrao* doctrine, the amendment should clarify that where a party can demonstrate that they made reasonable, documented efforts to obtain a certificate from a third-party system administrator but were unable to do so, the court may admit the electronic document if its authenticity and systemic reliability can be verified through alternative forensic means, such as hash-value validation or expert testimony.

B. Standardizing Digital Forensic Protocols

The Attorney-General of the Federation, in collaboration with agencies like NITDA and the National Security Adviser (NSA), should draft and gazette National Digital Forensic Operational Guidelines. These guidelines should be modeled after international standards, such as ISO/IEC 27037. By establishing mandatory rules for data seizure, imaging, and chain of custody documentation, the state can ensure that all digital evidence presented in court meets a uniform, scientifically verifiable threshold.

C. Accession to the Budapest Convention

Nigeria should pursue formal accession to the Council of Europe's Convention on Cybercrime (the Budapest Convention). Accession would grant domestic investigators access to expedited international cooperation networks, facilitating rapid data preservation requests and simplifying cross-border digital evidence recovery.

D. Judicial Capacity Building

The National Judicial Institute (NJI) should expand its continuing legal education programs to include specialized courses in digital forensics and cyber security for judicial officers. A judges' bench-book on electronic evidence should be developed to assist trial judges in evaluating complex digital evidence, metadata, cryptographic signatures, and synthetic media (such as deep fakes).

8. Conclusion

The introduction of Section 84 of the Evidence Act 2011 (as amended in 2023) and the enactment of the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 represented major steps forward for Nigeria's criminal justice system.However, the rapidly changing nature of digital technology has exposed gaps in these laws. The rigid insistence on formal paper certificates, combined with limited domestic forensic capabilities and slow international cooperation, continues to hinder cybercrime prosecutions.

Improving the administration of justice in this area requires more than simple statutory compliance. Nigeria must adopt a balanced approach that combines flexible legislative rules, standardized forensic practices, and stronger international partnerships. By implementing these practical reforms, Nigeria can build a resilient digital justice system capable of addressing modern cybercrime while respecting constitutional protections.

[23] *Case C-670/22, M.N. (EncroChat),* Judgment of the Court of Justice of the European Union (Grand Chamber), 30 April 2024.