



ADMISSIBILITY OF DIGITAL EVIDENCE IN CYBERCRIME PROSECUTION UNDER THE EVIDENCE ACT 2011

*Okorie, Hagler**

ABSTRACT

The emergence of information and communication technology has transformed the nature of criminal activities, giving rise to sophisticated cybercrimes such as hacking, identity theft, phishing, cyberstalking, online fraud, and unauthorized access to computer systems. As these offences are primarily committed through digital platforms, the successful prosecution of cybercrime cases largely depends on the admissibility and reliability of digital evidence. In Nigeria, the legal framework governing the admissibility of digital evidence is principally contained in the Evidence Act, 2011, particularly Section 84, which prescribes the conditions under which computer-generated evidence may be admitted in judicial proceedings. The enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 further strengthened the legal regime by recognizing electronic records and digital data as critical tools in the investigation and prosecution of cyber offences. This study examines the admissibility of digital evidence in cybercrime prosecution under the Evidence Act, 2011. It analyzes the concept and nature of digital evidence, the statutory requirements for its admissibility, and the judicial interpretation of Section 84 by Nigerian courts. The study also evaluates the significance of electronic records such as emails, text messages, computer logs, CCTV footage, social media communications, and digital forensic reports in proving cybercrime offences. Particular attention is given to the conditions relating to the regular use of computer systems, the reliability of the device used, and the requirement of certification for computer-generated evidence. The research identifies several challenges affecting the admissibility of digital evidence in Nigeria, including inadequate technical expertise among investigators and prosecutors, difficulties in maintaining the chain of custody of electronic evidence, issues of authenticity and integrity of digital records, and the strict procedural requirements imposed by Section 84 of the Evidence Act. Ultimately, the effective admissibility of digital evidence remains indispensable to the successful prosecution of cybercrime and the administration of criminal justice in Nigeria.

KEYWORDS: *Admissibility, Cybercrime, Cybercrime Prosecution, Digital Evidence and Electronic evidence.*

1. INTRODUCTION

The rapid advancement of information and communication technology (ICT) has significantly transformed modern society, creating unprecedented opportunities for communication, commerce, governance, and social interaction. However, these technological developments have also facilitated the emergence of cybercrime, which has become one of the most pervasive forms of transnational and domestic criminal activity in the twenty-first century. Cybercrime encompasses a wide range of unlawful activities committed through computers, computer networks, and digital devices, including hacking, identity theft, phishing, cyberstalking, online fraud, cyberterrorism,



and unauthorized access to protected systems.¹ As criminal activities increasingly migrate into the digital space, traditional forms of evidence are gradually being supplemented or replaced by electronic and digital evidence, making the admissibility of such evidence a critical issue in criminal prosecutions. Digital evidence refers to information of probative value that is stored, generated, transmitted, or received in electronic form and which may be relied upon in legal proceedings.² Such evidence may include emails, text messages, computer logs, metadata, digital photographs, CCTV recordings, social media communications, website records, call logs, electronic financial transactions, and forensic data recovered from digital devices. Unlike conventional documentary evidence, digital evidence possesses unique characteristics such as volatility, susceptibility to alteration, duplication, and ease of transmission, thereby necessitating special legal and procedural safeguards to ensure its authenticity and reliability.³

In Nigeria, the increasing prevalence of cybercrime has necessitated the development of legal frameworks capable of addressing both the substantive offences and the evidentiary challenges associated with digital technologies. The enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 represented a significant legislative response to the growing threat of cybercrime by criminalizing various cyber-related offences and empowering law enforcement agencies to investigate and prosecute offenders.⁴ However, the successful prosecution of cybercrime cases depends not merely on the existence of substantive criminal provisions but also on the ability of prosecutors to tender digital evidence in a manner consistent with the rules of evidence. Prior to the enactment of the Evidence Act, 2011, Nigerian courts faced considerable difficulties in admitting computer-generated evidence because the Evidence Act, 1945 did not contain express provisions regulating electronic evidence. Consequently, litigants often encountered challenges in establishing the admissibility and authenticity of electronically generated documents.⁵ Recognizing the inadequacy of the previous legal regime, the legislature introduced the Evidence Act, 2011, which revolutionized the law of evidence in Nigeria by expressly recognizing the admissibility of computer-generated evidence through Section 84 of the Act.⁶ This provision marked a significant departure from the traditional common law approach and aligned Nigerian evidentiary law with international best practices concerning electronic evidence. *Section 84* of the Evidence Act, 2011 provides the statutory conditions under which statements contained in documents produced by computers may be admitted in evidence. The section requires proof that the computer was regularly used to store or process information during the relevant period, that the information was supplied

* Ph.D, FCARB, FICMC is a Notary Public and Justice of Peace. He is the Head of Department, Private and Property Law (PPL) at the Faculty of Law, Abia State University, Umahia Campus; 08032253813, haglersoco@gmail.com; hagler.okorie@abiastateuniversity.edu.ng.

¹ Convention on Cybercrime, art 1; Yinka Akinseye-George, *The Law of Cybercrimes in Nigeria*, Princeton Publishing Co, 2018, 3.

² S Mason, *Electronic Evidence*, 5th edn, Institute of Advanced Legal Studies 2021, 6.

³ P R Rice, *Electronic Evidence: Law and Practice*, American Bar Association, 2019, 12.

⁴ Cybercrimes (Prohibition, Prevention, etc.) s 1-58.

⁵ M T Ladan, *Materials and Cases on Nigerian Law of Evidence*, Ahmadu Bello University Press, 2016, 412.

⁶ Evidence Act 2011, s 84.



in the ordinary course of activities, that the computer was operating properly, and that a certificate identifying the document and describing the manner of its production accompanies the evidence.⁷ These requirements are intended to guarantee the authenticity, reliability, and integrity of computer-generated evidence before it is admitted by the courts.

The interpretation and application of Section 84 have generated considerable judicial discourse in Nigeria. In *Dickson v. Sylva & Ors*,⁸ the Supreme Court emphasized the necessity of complying with the conditions stipulated under Section 84 before computer-generated evidence can be admitted. Similarly, in *Kubor v Dickson*,⁹ the Supreme Court underscored the mandatory nature of the certification requirement and reaffirmed that electronic documents must satisfy the statutory conditions for admissibility. These judicial decisions demonstrate the courts' commitment to ensuring that digital evidence admitted in legal proceedings possesses sufficient guarantees of authenticity and reliability. Notwithstanding the legislative recognition of digital evidence, several challenges continue to impede its effective utilization in cybercrime prosecutions. These challenges include inadequate digital forensic infrastructure, insufficient technical expertise among investigators and prosecutors, difficulties in maintaining the chain of custody of electronic evidence, risks of data manipulation, cross-border jurisdictional issues, and strict compliance requirements under Section 84 of the Evidence Act. Furthermore, the dynamic nature of technology often outpaces legal and institutional responses, thereby creating uncertainties in the application of existing evidentiary rules to emerging forms of digital evidence. The importance of digital evidence in cybercrime prosecution cannot be overstated. Given that cybercrimes are predominantly committed through electronic means, digital evidence often constitutes the primary or sole basis upon which guilt or innocence may be established. Consequently, the effectiveness of the criminal justice system in combating cybercrime depends largely on the adequacy of legal rules governing the admissibility, authentication, preservation, and evaluation of electronic evidence.¹⁰

2. CONCEPTUAL CLARIFICATION

a. Admissibility of Evidence

Admissibility refers to the legal acceptability of evidence before a court of law. Evidence is admissible when it satisfies the requirements prescribed by law and is relevant to the facts in issue before the court.¹¹ Under Nigerian law, admissibility generally depends on relevance, legality, and compliance with statutory provisions governing the particular category of evidence sought to be tendered.¹² The Supreme Court in *Torti v Ukpabi*,¹³ stated that the primary test for admissibility is

⁷ EA 2011 s 84(2)-(4).

⁸ (2016) LPELR-41257(SC).

⁹ (2012) LPELR-15364(CA).

¹⁰ M Ozekhome, *Cybercrime and Electronic Evidence in Nigeria*, (Malthouse Press Ltd, 2021) 87

¹¹ F Nwadialo, *Modern Nigerian Law of Evidence*, 2nd edn, University of Lagos, Press 1999, 15.

¹² Evidence Act 2011, s 1-3.

¹³ (1984) 1 SCNLR 214.



relevance. However, where legislation prescribes specific conditions for admissibility, such conditions must also be satisfied before the evidence can be admitted. In the context of digital evidence, admissibility requires compliance with the provisions of Section 84 of the Evidence Act, 2011, which establishes special conditions for the admission of computer-generated evidence.

b. Cybercrime

Cybercrime refers to criminal activities carried out through the use of computers, digital devices, computer networks, or the internet. It includes offences in which computers or information systems serve either as the target of the offence or as the instrument through which the offence is committed.¹⁴ The Cybercrimes (Prohibition, Prevention, etc.) Act does not provide a comprehensive definition of cybercrime but criminalizes numerous acts such as unlawful access to computer systems, computer-related fraud, identity theft, cyberstalking, cybersquatting, electronic forgery, child pornography, and cyberterrorism.¹⁵ The Convention on Cybercrime describes cybercrime broadly as offences committed against the confidentiality, integrity, and availability of computer systems, networks, and electronic data.¹⁶ Cybercrime differs from conventional crime because it is often transnational, anonymous, technologically sophisticated, and capable of affecting numerous victims simultaneously.¹⁷

c. Cybercrime Prosecution

Cybercrime prosecution refers to the process through which individuals or organizations accused of committing cyber-related offences are investigated, charged, tried, and punished in accordance with applicable laws. It involves the collection, preservation, authentication, and presentation of digital evidence before a court for the purpose of establishing criminal liability. Successful cybercrime prosecution depends heavily on digital forensic investigations and the admissibility of electronic evidence because cyber offences often leave electronic traces rather than physical evidence. Investigative agencies such as the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force, and Independent Corrupt Practices and Other Related Offences Commission (ICPC) frequently rely on digital evidence recovered from computers, mobile devices, servers, and online platforms to establish guilt in cybercrime cases.¹⁸

d. Digital Evidence

Digital evidence refers to information or data of probative value that is stored, transmitted, generated, received, or preserved in electronic form and can be used in legal proceedings to establish facts in issue.¹⁹ It encompasses any information extracted from electronic devices such as

¹⁴ Y Akinseye-George, *The Law of Cybercrimes in Nigeria*, (Princeton Publishing Co. 2018) 5.

¹⁵ Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 6-39.

¹⁶ Convention on Cybercrime 2001, art 2-11.

¹⁷ Jonathan, C., *Principles of Cybercrime*, 3rd edn, (Cambridge University Press, 2021) 14.

¹⁸ Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 38 -41.

¹⁹ S Mason, *Electronic Evidence* 6.



computers, mobile phones, tablets, servers, digital cameras, automated teller machines (ATMs), cloud storage systems, and internet platforms. Unlike traditional documentary evidence, digital evidence exists in intangible electronic formats and often requires specialized tools and expertise for its identification, preservation, extraction, and analysis.²⁰ According to Stephen Mason, digital evidence consists of information generated, stored, or communicated by electronic devices which may be relied upon before a court of law to prove or disprove a material fact.²¹ Such evidence may include emails, text messages, social media posts, digital photographs, audio recordings, video recordings, internet browsing histories, metadata, GPS records, call logs, electronic bank records, and forensic images obtained from digital devices.²² The relevance of digital evidence has increased significantly due to the proliferation of cybercrimes and the growing reliance on electronic communication in commercial and social interactions. Consequently, modern criminal investigations frequently depend on digital evidence as a primary source of proof.

e. Electronic Evidence

Electronic evidence is a broad category of evidence that includes all information created, stored, communicated, or received in electronic form. The term is often used interchangeably with digital evidence, although electronic evidence may include both digital and analogue electronic records.²³ Electronic evidence comprises emails, computer-generated documents, electronic contracts, CCTV recordings, text messages, social media communications, call detail records, electronic signatures, electronic payment records, and data generated by information systems.²⁴ The Evidence Act, 2011 recognizes electronic records as documents capable of being admitted in evidence, provided the conditions stipulated under the Act are satisfied.²⁵ The recognition of electronic evidence reflects the realities of contemporary technological advancements and electronic transactions.

3. ADMISSIBILITY OF DIGITAL EVIDENCE IN CYBERCRIME PROSECUTION UNDER THE EVIDENCE ACT, 2011

The prosecution of cybercrime offences is heavily dependent on digital evidence because most cybercrimes are committed through electronic devices, computer systems, and internet-based platforms. Unlike conventional crimes where physical evidence such as weapons, fingerprints, or documents may be available, cybercrime investigations often rely on electronic records, computer-generated documents, emails, call logs, social media communications, server records, IP addresses, CCTV footage, digital photographs, metadata, and forensic reports recovered from digital devices.²⁶ Consequently, the admissibility of digital evidence has become a critical aspect of criminal justice administration in Nigeria. The enactment of the Evidence Act, 2011 marked a

²⁰ E Casey, *Digital Evidence and Computer Crime*, (4th edn, Academic Press, 2020) 23.

²¹ S Mason, (n 11) 8.

²² E Casey, (n 12) 31.

²³ G L Paul, *Foundations of Digital Evidence*, American Bar Association, 2017, 11.

²⁴ S Mason, (n 11) 19.

²⁵ Evidence Act 2011, s 94 and 258.

²⁶ E Casey, *Digital Evidence and Computer Crime* 25.

significant turning point in Nigerian evidentiary law by expressly recognizing the admissibility of electronic and computer-generated evidence. Before the enactment of the Act, courts faced difficulties admitting electronic records because the Evidence Act, 1945 contained no specific provisions governing digital evidence. The Evidence Act, 2011 addressed this gap by introducing Section 84, which provides a comprehensive framework for the admissibility of computer-generated evidence.

3.1 Meaning and Importance of Digital Evidence in Cybercrime Prosecution

Digital evidence refers to information stored or transmitted in binary form that may be relied upon before a court to prove or disprove a fact in issue. Such evidence may originate from computers, smartphones, tablets, servers, cloud storage systems, websites, email accounts, social media platforms, automated teller machines (ATMs), and other electronic devices. In cybercrime prosecutions, digital evidence serves several important functions. First, it assists investigators in identifying suspects through IP addresses, login credentials, electronic transaction records, and communication logs.²⁷ Second, it establishes the occurrence of criminal activities such as unauthorized access, phishing, identity theft, cyberstalking, and electronic fraud. Third, it links suspects to criminal conduct through forensic analysis of digital devices and electronic records. Given that cybercrime offences are largely committed in virtual environments, digital evidence often constitutes the primary evidence upon which convictions are secured.

4. STATUTORY FRAMEWORK FOR ADMISSIBILITY OF DIGITAL EVIDENCE UNDER THE EVIDENCE ACT, 2011

The principal statutory provision governing the admissibility of digital evidence in Nigeria is *Section 84* of the Evidence Act, 2011. The provision creates an exception to the traditional hearsay rule by permitting the admission of statements contained in documents produced by computers.

Section 84(1) provides that:

In any proceeding, 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.

The significance of this provision lies in its recognition that computer-generated documents are capable of being admitted as evidence despite the absence of direct human authorship. The section therefore legitimizes the use of electronic records such as emails, electronic bank statements, text messages, website records, digital photographs, CCTV recordings, and social media communications in criminal proceedings.

²⁷ Y Akinseye-George, *The Law of Cybercrimes in Nigeria* 84.



4.1 Conditions for Admissibility under Section 84(2):

Section 84(2) prescribes specific conditions that must be satisfied before computer-generated evidence can be admitted in court.

(a) Regular Use of the Computer

The computer used to generate or store the information must have been regularly used during the relevant period for activities carried out by a person having lawful control over its operation. This requirement seeks to establish the reliability and authenticity of the computer system by demonstrating that it was routinely used in the ordinary course of business or official activities rather than being specially prepared for litigation.

(b) Information Supplied in the Ordinary Course of Activities

The information contained in the electronic record must have been supplied to the computer during the ordinary course of activities. The rationale behind this requirement is to ensure that the information was generated as part of normal operations and not fabricated for evidential purposes.

(c) Proper Functioning of the Computer

The applicant must establish that the computer was operating properly throughout the material period or that any malfunction did not affect the accuracy of the information produced. This requirement is crucial because digital systems may experience technical failures capable of compromising the reliability of stored data.²⁸

(d) Information Derived from Data Supplied to the Computer

The information contained in the document must be derived from data supplied to the computer in the ordinary course of activities. The purpose is to ensure that the information presented before the court is traceable to legitimate sources and has not been manipulated.

4.2 Certificate Requirement under Section 84(4)

One of the most important requirements for admissibility is the certificate prescribed by *Section 84(4)* of the Evidence Act.

The certificate must:

1. Identify the electronic document;
2. Describe the manner in which it was produced;
3. Provide particulars of the device involved in producing the document;
4. Certify compliance with the requirements of Section 84(2); and
5. Be signed by a person occupying a responsible position in relation to the operation of the relevant device or management of the relevant activities.

²⁸ Casey (n 1) 85.



The certificate serves as proof of authenticity and reliability of the electronic evidence. It also assists the court in determining whether the statutory conditions have been fulfilled.

4.3 Judicial Interpretation of Section 84

Nigerian courts have delivered several landmark decisions concerning the admissibility of digital evidence.

a. *Kubor v Dickson*

In *Kubor v Dickson*,²⁹ the Supreme Court held that documents generated from a computer system are inadmissible unless the requirements of Section 84 are satisfied. The Court emphasized that compliance with the statutory conditions is mandatory and that parties seeking to rely on computer-generated evidence must demonstrate conformity with the provisions of the Act. This decision established the foundational principle that electronic evidence cannot be admitted merely because it is relevant; compliance with Section 84 remains indispensable.

b. *Dickson v Sylva & Ors*

In *Dickson v Sylva & Ors*,³⁰ the Supreme Court reaffirmed the mandatory nature of Section 84 and stressed that electronic documents must satisfy all statutory requirements before admission. The Court observed that failure to provide the certificate required under Section 84(4) may render the evidence inadmissible.

c. *FRN v Fani-Kayode*

In *FRN v Fani-Kayode*,³¹ the court recognized the growing importance of electronic evidence in criminal proceedings and underscored the need for compliance with statutory safeguards to guarantee authenticity and reliability. The decision illustrates the judiciary's willingness to admit digital evidence where the requirements of the Evidence Act are properly observed.

5. TYPES OF DIGITAL EVIDENCE COMMONLY ADMITTED IN CYBERCRIME CASES

Various forms of digital evidence are admissible under the Evidence Act, provided the requirements of Section 84 are fulfilled. These include:

a. Emails

Emails frequently serve as evidence of fraudulent communications, conspiracy, phishing schemes, and unauthorized transactions.

²⁹ *Supra.*

³⁰ *Supra.*

³¹ (2019) LPELR-87065 CA



b. Text Messages and Instant Messaging Records

SMS messages, WhatsApp chats, Telegram communications, and other electronic messages are regularly relied upon to establish criminal intent, participation, and communication among suspects.

c. Social Media Records

Posts, comments, messages, videos, and photographs obtained from social media platforms such as Facebook, X (formerly Twitter), Instagram, and TikTok may be tendered as evidence in cybercrime prosecutions.

d. CCTV Footage and Digital Photographs

Video recordings and photographs generated by surveillance systems often provide visual proof of criminal conduct.

e. Bank Transaction Records

Electronic banking records and payment histories are essential in prosecuting offences involving online fraud, identity theft, money laundering, and electronic theft.

6. CHALLENGES AFFECTING THE ADMISSIBILITY OF DIGITAL EVIDENCE

Despite the statutory framework established by the Evidence Act, several challenges continue to affect the admissibility of digital evidence in Nigeria.

a. Technical Complexity

Judges, prosecutors, and lawyers may lack sufficient technical expertise to understand sophisticated digital evidence and forensic methodologies.

b. Chain of Custody Problems

Failure to maintain a proper chain of custody may create doubts regarding the authenticity and integrity of electronic evidence.

c. Data Manipulation and Alteration

Digital evidence can be altered, deleted, fabricated, or manipulated with relative ease, raising concerns regarding authenticity and reliability.

d. Compliance with Section 84

Strict compliance with Section 84 often creates procedural difficulties, particularly where investigators fail to obtain the required certificate at the time evidence is collected.

e. Cross-Border Nature of Cybercrime

Many cybercrimes involve foreign servers, multinational service providers, and transnational offenders, making it difficult to obtain electronic evidence and satisfy evidentiary requirements under Nigerian law.

7. IMPACT OF THE EVIDENCE ACT, 2011 ON CYBERCRIME PROSECUTION

The Evidence Act, 2011 has significantly enhanced the prosecution of cybercrime offences by formally recognizing digital evidence as admissible evidence in judicial proceedings.³² The Act has provided legal certainty regarding the admissibility of computer-generated documents and has enabled law enforcement agencies to rely on electronic records in proving cyber-related offences.³³ Furthermore, the Act has aligned Nigeria's evidentiary regime with international standards governing electronic evidence and digital investigations.³⁴ By establishing safeguards aimed at ensuring authenticity, reliability, and integrity, the Act balances the need for technological adaptation with the protection of fair trial rights.

8. RECENT LEGISLATIVE DEVELOPMENTS INTRODUCED BY THE EVIDENCE (AMENDMENT) ACT, 2023

The enactment of the Evidence (Amendment) Act, 2023 represents one of the most significant reforms of Nigeria's law of evidence since the enactment of the Evidence Act, 2011. The Amendment Act was assented to on 12 June 2023 with the primary objective of aligning Nigerian evidentiary rules with contemporary technological advancements and the realities of digital communication, electronic transactions, and virtual judicial proceedings. The Act introduced several innovations aimed at expanding the admissibility, authentication, and evidential value of electronic records in judicial proceedings. It particularly strengthened the legal framework governing digital evidence, thereby enhancing the prosecution of cybercrime and other technology-related offences.

a. Expansion of Section 84 to Cover Electronic Records

One of the most important amendments introduced by the Evidence (Amendment) Act, 2023 is the expansion of Section 84 of the Evidence Act, 2011 to expressly include **electronic records** in addition to computer-generated documents. Prior to the amendment, Section 84 primarily referred to "documents produced by a computer." The amendment inserted the phrase "or electronic records" into the provision, thereby widening the scope of admissible electronic evidence. This amendment is particularly significant because modern digital information is often stored and transmitted through cloud computing platforms, mobile applications, social media platforms, and online databases rather than through traditional computer printouts. Consequently, electronic records such

³² Evidence Act, 2011, s 84.

³³ Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

³⁴ Convention on Cybercrime 2001, art 14-21.



as emails, WhatsApp messages, metadata, cloud-based documents, electronic images, and audio recordings now fall more clearly within the ambit of admissible evidence.

b. Introduction of a Statutory Definition of Electronic Records

The Amendment Act introduced a comprehensive definition of "electronic record." Under the amended law, an electronic record includes data, records, images, sound, or information generated, stored, received, or transmitted electronically, including those stored in microfilm or other electronic formats. This definition removes uncertainties regarding the status of various forms of electronically stored information and reflects international best practices in electronic evidence law. It also ensures that courts can accommodate emerging technologies and digital communication methods without requiring further legislative intervention.

c. Insertion of New Sections 84A–84D

The Amendment Act introduced four new provisions—Sections 84A, 84B, 84C, and 84D—which collectively establish a modern legal framework for electronic evidence and digital transactions.

(i) Section 84A: Recognition of Electronic Documents

Section 84A provides that where any law requires information to be in writing, typewritten, or printed form, such requirement shall be satisfied if the information is rendered in an electronic form that is accessible for future reference. This provision grants electronic documents the same legal status as paper documents and facilitates the admission of electronic communications in judicial proceedings.

(ii) Section 84B: Admissibility of Electronic Signatures

Section 84B recognizes electronic signatures as legally valid means of authenticating electronic records and transactions. The provision establishes a presumption that electronic signatures attached to electronic records are valid unless the contrary is proved. This innovation is particularly relevant in electronic commerce, online banking, digital contracts, and cybercrime investigations where the authenticity of electronic communications is often in issue.

(iii) Section 84C: Authentication of Electronic Records

Section 84C establishes presumptions regarding the authenticity and integrity of electronic records generated or maintained in secure electronic systems. The provision simplifies the burden of proving the reliability of certain electronic records and enhances the efficiency of judicial proceedings involving digital evidence.

(iv) Section 84D: Presumption as to Secure Electronic Records

Section 84D introduces legal presumptions regarding secure electronic records and secure electronic signatures. The provision empowers courts to presume that secure electronic records have not been altered since the specific point in time to which the security status relates unless

evidence is produced to the contrary. This provision is particularly important in cybercrime prosecutions where challenges relating to data integrity and authenticity frequently arise.

d. Recognition of Cloud-Based and Digitally Stored Information

The Amendment Act significantly broadened the categories of electronic evidence that may be admitted by recognizing records stored in cloud computing environments, optical media, magnetic storage devices, and other electronic databases. Electronic records stored remotely are now capable of admission without the stringent requirement of producing original paper copies, provided statutory conditions are met. This development is particularly beneficial in cybercrime investigations because many digital communications and transactional records are now stored on remote servers located within and outside Nigeria.

e. Recognition of Electronic Oath-Taking and Virtual Proceedings

The Amendment Act introduced provisions accommodating electronic oath-taking and other digital procedures connected with virtual court proceedings. These reforms were influenced by the increasing use of remote hearings and technology-assisted judicial processes, particularly following experiences during and after the COVID-19 pandemic.³⁵ The innovation enhances access to justice, reduces delays, and aligns judicial practice with modern technological realities.

9. CONCLUSION

The admissibility of digital evidence has become an indispensable component of cybercrime prosecution in Nigeria due to the increasing dependence on information and communication technologies in both lawful and criminal activities. Since cybercrimes are predominantly committed through electronic platforms, digital evidence often constitutes the primary means through which investigators identify suspects, establish criminal conduct, and secure convictions. Consequently, the effectiveness of cybercrime prosecution is closely linked to the legal framework governing the admissibility, authentication, and evaluation of electronic evidence. The Evidence Act, 2011, particularly Section 84, marked a significant milestone in Nigerian evidentiary law by expressly recognizing the admissibility of computer-generated evidence and establishing conditions designed to ensure the authenticity and reliability of electronic records. Judicial decisions such as *Kubor v Dickson* and *Dickson v. Sylva & Ors* have further clarified the requirements for admitting digital evidence, emphasizing strict compliance with statutory provisions. These developments have provided courts with a structured legal basis for assessing the evidential value of electronic records in both civil and criminal proceedings. Furthermore, the enactment of the Evidence (Amendment) Act, 2023 has modernized Nigeria's law of evidence by expanding the scope of admissible electronic records, recognizing electronic signatures, validating cloud-based data, introducing presumptions relating to secure electronic records, and accommodating technological innovations in judicial proceedings. These reforms have

³⁵ Evidence (Amendment) Act, 2023, s 108-110.



strengthened the legal framework for handling digital evidence and have brought Nigerian evidentiary law closer to international best practices in electronic evidence and cybercrime prosecution.

Notwithstanding these legislative advancements, significant challenges remain. Issues relating to technical expertise, digital forensic capacity, preservation of electronic evidence, chain of custody, cross-border investigations, and compliance with statutory certification requirements continue to affect the effective utilization of digital evidence in criminal proceedings. The rapid evolution of technology also poses continuous challenges to legal institutions and law enforcement agencies tasked with investigating and prosecuting cybercrime. In conclusion, while the Evidence Act, 2011 and the Evidence (Amendment) Act, 2023 provide a robust legal foundation for the admissibility of digital evidence in Nigeria, the success of cybercrime prosecution ultimately depends on the effective implementation of these provisions. Strengthening institutional capacity, enhancing digital forensic infrastructure, promoting specialized training for investigators, prosecutors, and judicial officers, and ensuring continuous legislative adaptation to emerging technologies are essential for maintaining the integrity and effectiveness of the criminal justice system in the digital age. Through these measures, digital evidence will continue to serve as a vital tool in combating cybercrime and promoting the administration of justice in Nigeria.

10. RECOMMENDATIONS

Based on the findings of this study on the Admissibility of Digital Evidence in Cybercrime Prosecution under the Evidence Act, 2011, the following recommendations are proposed:

1. Continuous Review of the Evidence Act and Cybercrime Laws

Given the rapid evolution of technology, the National Assembly should periodically review and update the provisions of the Evidence Act and the Cybercrimes (Prohibition, Prevention, etc.) Act to address emerging forms of digital evidence and cybercrime techniques. Legislative reforms should ensure that evidentiary rules remain responsive to technological advancements such as artificial intelligence, blockchain technology, cryptocurrency transactions, cloud computing, and digital forensics.

2. Simplification of the Requirements under Section 84 of the Evidence Act

While Section 84 of the Evidence Act provides safeguards for the authenticity of electronic evidence, its procedural requirements, particularly the certification requirement, may sometimes create unnecessary technical obstacles to the admission of relevant evidence. The legislature should consider introducing clearer and more flexible procedures that preserve the integrity of electronic evidence without frustrating the administration of justice through excessive technicalities.



3. Capacity Building for Judges and Judicial Officers

Regular training programmes should be organized for judges, magistrates, and other judicial officers on digital technology, electronic evidence, cybercrime investigations, and digital forensic processes. This will enhance their ability to properly evaluate the authenticity, reliability, and probative value of electronic evidence presented before the courts.

4. Specialized Training for Prosecutors and Investigators

Law enforcement officers, prosecutors, and investigators should receive continuous professional training in cybercrime detection, digital evidence collection, preservation, analysis, and presentation. Specialized knowledge will reduce errors in handling electronic evidence and improve compliance with statutory requirements governing admissibility.

5. Strengthening Digital Forensic Infrastructure

Government should invest in modern digital forensic laboratories and technological infrastructure to support cybercrime investigations. Agencies such as the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force, and Independent Corrupt Practices and Other Related Offences Commission (ICPC) should be equipped with advanced forensic tools capable of extracting, preserving, and analysing electronic evidence in accordance with international standards.