Scientific Research Publishing

Beijing Law Review, 2025, 16(2), 1037-1049
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Cybercrime and Digital Transactions Law in Nigeria towards Attainment of Sustainable Development Goals

Ngozi Chisom Uzoka[1*], Nneka Obiamaka Umejiaku[1], Anthony Chinedu Onah[2], Chidimma Stella Nwakoby[3], Onyekachukwu Ijeoma Eze[4]

[1]Department of Private & Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria
[2]Department of Clinical Legal Education, Nnamdi Azikiwe University, Awka, Nigeria
[3]Department of Commercial and Property Law, Faculty of Law, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Nigeria
[4]Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria
Email: nc.uzoka@unizik.edu.ng, ngoziuzoka4@gmail.com, *no.umejiaku@unzik.edu.ng, ac.onah@unzik.edu.ng, cs.nwakoby@coou.edu.ng, onyekachukwu.eze120@gmail.com

How to cite this paper: Uzoka, N. C., Umejiaku, N. O., Onah, A. C., Nwakoby, C. S., & Eze, O. I. (2025). Cybercrime and Digital Transactions Law in Nigeria towards Attainment of Sustainable Development Goals. *Beijing Law Review, 16,* 1037-1049.
https://doi.org/10.4236/blr.2025.162053

Received: May 1, 2025
Accepted: June 22, 2025
Published: June 25, 2025

Abstract

Objective of Study: The paper aims to identify the relevance, authenticity, and nexus between digital transactions and cybercrime laws and how they affect sustainable development strides in Nigeria. This paper seeks to give a summary of cybercrime and digital transaction laws in Nigeria, as well as the challenges inherent in applying them. **Method:** The study adopted the doctrinal method of legal research approach in literature review, analysis of cases, and access to internet sources. This paper also made use of primary sources of data such as enabling laws, acts, secondary sources of data, conventions, and journal articles, and the study is also analytical and comparative in nature. **Theoretical Framework:** Routine activity theory posits that cybercrime is more likely to take place when there is a convergence of a motivated offender, a suitable target (e.g., computer system, data), and the absence of capable guardianship (e.g., security measures). Cybercriminals often exploit vulnerabilities in computer systems and networks, targeting valuable data or systems where security is weak. Another theory is the social learning theory, which was propounded by Albert Bandura. The social learning theory is based upon the influence of the actors in the social environment on an individual to perpetrate a crime. The actors in the social environment here are deviant peers who can share negative influence and can be imitated in society. Cybercrime activity involves a required level of competence in the knowledge of computers to be able to use it to perpetrate crime, and this can only be acquired by imitating deviant individuals who have mastered criminal acts. The proponents of the social learning theory have for-

mulated four processes in explaining this theory, which are differential association, definitions, differential reinforcement, and imitation. A motivation to commit cybercrime begins with close association and mingling with deviant peers in society who have mastered the acts of using computers to commit crimes through online activity. Other individuals in society observe these cybercriminals and are motivated probably because of the lack of apprehension and ostentatious lifestyle they live. This is the point where imitation begins. **Result:** The study finds that the legal and institutional framework for digital transaction laws in Nigeria is somewhat limited. Some digital forensic tools have not been recognized by our laws in Nigeria. The paper finds that cybercrime causes reputational damage to a country and destroys the domestic economy, reducing the competitive advantages of a nation for socio-economic development. The paper concludes that the extant legal framework for digital transaction laws in Nigeria has lapses that impair the evidence emanating from digital tools/records. This paper recommends, amongst others, training of prosecution officers, legal practitioners, and judicial officers in the collection and use of forensic/digital evidence in court of law, review of some of our extant laws, and creation of an institutional framework for digital transaction laws in Nigeria.

Keywords

Digital Law, Cybercrime, Justice, Electronic Law, Electronic Evidence, E-Commerce, SDGs

1. Introduction

Two decades ago, many people did not have mobile phones or computers because of the cost. Connecting to the internet was only accessible through dial-up modems. In Nigeria, before now, people paid hourly or by minute to access the internet in cybercafes. The use of electronic mail was not common, and neither was the use of electronic banking systems. Presently, many individuals now own laptops or mobile phones that can connect to the internet and email accounts effortlessly wherever they are. Presently, there are many social media platforms where people can connect easily with others without physically meeting. Individuals now frequently purchase goods online and are increasingly using electronic readers for books and newspapers rather than traditional print media. On the other hand, Sustainable Development Goals (SDGs) were adopted by the United Nations in 2015 as a universal call to action to end poverty, protect the planet, and ensure that by 2030, people enjoy peace and prosperity all over the world.

Over two decades, there has been an increased usage of technological inventions, which has provided a platform for its misuse and crimes. This has increased the use of technology by individuals to create new forms of crime. With the emergence of information and communication technology and the growing usage of the internet on a daily basis, there are now many avenues through which cybercrimes can be carried out. "Individuals who engage in socially unacceptable or

outright criminal acts steadily make use of technology to connect with one another in ways that are not before now possible." (Holt, Bossler, & Seigfried-Spellar, 2015). Because of the possibility of carrying out transactions online without any physical meeting, persons have taken undue advantage of that to perpetuate and engage in all sorts of cybercrimes. As a result of the differences in jurisdictions, there is no generally acceptable definition of cybercrime that is all-encompassing. Cybercrime is challenging to conceptualize with exactitude. However, one factor remains constant in various definitions given by scholars. Cybercrime is a crime that is committed over the wireless internet. On the other hand, cybercrime can be termed as any crime or criminal activity executed by making use of digital technology, or put differently, they are computer-related crimes and crimes related to the internet. Digital technology and electronic networks provide an enviable platform to promote commercial transactions across the globe. A major sector of the economy that has robustly been affected positively or negatively by the intrusion of digital technology is the banking sector. Digital banking has facilitated a great deal of digital transactions; hence, sellers and buyers of goods and services leverage digital technology to initiate and conclude their transactions without any physical meeting. In a society where cyberattacks grow in scale and frequency, the societal structures needed to foster sustainable development goals will be the victims. Consequently, it will undermine progress toward all goals, particularly goal 16, which provides for Peace, Justice, and Strong Institutions. Thus, it is without doubt that in Nigeria and the world at large, financial technology has provided a formidable platform for digital banking operators to provide a wide range of financial services. This has, in turn, opened the door for an influx of various types of cybercrimes. Additionally, collaborative efforts among nations need secure data sharing to achieve the SDGs while addressing concerns about data privacy, ownership, and misuse.

Cybercrimes and cyberattacks not only pose immediate threats to individuals' digital identities and financial well-being but also extend their influence on the stability of nations and the integrity of democratic processes. The significance of cybersecurity is growing, impacting individuals, entities, and entire countries. Malicious online activities, including cyberattacks, have the potential to jeopardize confidential data, interrupt public services, and inflict economic damage. (Agubo-shim, Obiokafor, & Emenike, 2023)

2. The Relevance of Digital Transactions to Cybercrime

Owing to the internet's globalization and the trans-border nature of digital transactions, cybercrime can occur anywhere. It suffices to state that there would be no cybercrime, if there was no internet. With the ease and access to the internet by all and sundry in Nigeria, coupled with the availability of different network providers of internet accessibility, digital transactions are on the increase. Years back, the main medium of payment in Nigeria was basically cash. This has led to a lot of vulnerabilities and losses caused by robbery, theft, etc. Subsequently, banks and other businesses introduced the use of Automated Teller Machines (ATM), Point

of Sales (POS), and bank apps. (Digital Payments in Nigeria, 2024) Cybercriminals in Nigeria are exploiting the widespread use of mobile banking apps and online payment platforms. Their tactics range from phishing and SIM swap fraud to ransomware attacks targeting banking institutions. As more people make use of the internet to transact business or make payments, there is a higher risk of being victims of cyber-attacks like online fraud, identity theft (Hoar, 2001), and spyware or virus attacks. (Rathna et al., 2023) The faster the adoption of new payment systems, the more rapid and sophisticated the cyber risks are. A secured payment is paramount for any business that relies on electronic payments and transactions. If the digital payment system is weak, then it will be prone to constant attacks by cybercriminals. The negative consequences of cybercrime are vast and are a growing cause of global concern. The COVID-19 pandemic also helped businesses to digitize their products and services, migrate to electronic commerce platforms, and leverage online business continuity strategy.

Cybercrime is evident not only in Nigeria but also in the world as a global menace. Studies have estimated a yearly 15 per cent increase in global cybercrime losses over the next five years, reaching 10.5 trillion US Dollars annually by 2025 (Businessday Newspaper Nigeria, 2022). In Nigeria, over 2800 persons were convicted of cybercrime in 2022 (Queen Troanusi, 2022). The increase in cybercrimes in Nigeria is highly attributed to the development and improvement of the internet. The development of the Electronic Data Interchange, which replaced the traditional mailing of documents with a digital transfer of data from one computer to another, enhances the transfer of orders and other transactions. Thus, EDI allows the transfer of data seamlessly without any human intervention. With digital transactions, people can transact business from any part of the world without really verifying the authenticity of the other party. This is a major threat to transacting business electronically/digitally. On the other hand, electronic/digital transaction platforms provide the buyer and the seller with a wide range of databases of services and products from which to choose within a short time. It also eliminates the need for an agent or middleman; this will, in turn, reduce to some extent the risk of counterfeit and adulterated products as there is a direct channel between the producer and the consumer.

3. Digital Transactions in Nigeria

Generally, a lot of services or goods can be rendered or purchased digitally. Thus, an electronic transaction is the buying and selling of goods and services online. Additionally, conducting major and essential elements of a contract or any business, whether commercial or non-commercial in nature, via communications transmitted through digital devices will qualify the transaction as an electronic one. The term digital transaction can be used interchangeably with the term 'electronic commerce'. Electronic commerce has no universal definition. However, it has been defined as commercial transactions conducted electronically on the internet. (OECD, 1997) In Nigeria, the total transaction value in the digital payments mar-

ket is projected to reach US $21.32bn in 2024. Presently, Nigeria's digital transactions revolution is driving economic growth and financial inclusion at unprecedented levels (AU Worldwide, 2022). While cash is still in use in Nigeria, there is a paradigm shift towards the adoption of digital payment systems. It is proven through research that governments that advance their national payment system create an enabling environment for everyone in the payments. There are several risks that organizations involved in electronic commerce encounter, such as financial, legal, supply chain, safety, and security. The security risk presents several components or dimensions. One of the most concerning is the cybersecurity risk. The high level of interconnectivity, which characterizes modern society and international trade, has opened many avenues for cyber-attacks, rendering cybersecurity an issue of major concern for all organizations (World Economic Forum, 2018).

4. Digital Transactions Regulation in Nigeria

Legal Framework for Cybercrimes and Digital Transactions in Nigeria

Digital or electronic transactions have raised a lot of novel issues with respect to control and regulation. The issue of validity, security, and enforceability of digital transactions is vital.

1) Evidence (Amendment Act) 2023

Evidence Act is one of the principal legislations used in Nigerian courts. It has been subject to some amendments as a result of the evolving legal system and the need to keep up with international best practices. The Evidence (Amendment) Act of 2023 brought significant changes in Nigeria's legal jurisprudence. However, it remained largely unchanged with respect to the inadmissibility of electronically generated evidence. Hence, there was a need to address the lacuna in the Act to reflect technological realities in the world today. Under the erstwhile Evidence Act of 2011, the admissibility of computer-generated evidence was introduced under Section 84. The 2011 Act also defined a document as including any device by means of which information is recorded, stored, or retrievable, including computer output (Section 258). However, more was needed to improve the admissibility of evidence, particularly electronically generated evidence, as contained in the Evidence Act of 2011. Hence, the Evidence (Amendment) Act of 2023 introduced novel digital and electronic execution of documents and the admissibility of storage mediums as evidence.

The Evidence (Amendment) Act of 2023 indeed contains visible provisions geared towards the digitization of transactions and processes, which will find expression in various fields and sectors, ranging from business contracts, financial transactions, government documents, and healthcare records. The federal government in Nigeria, in its bid to combat the overwhelming increasing rage of cybercrimes in Nigeria and protect the digital space, has enacted a few legislations in this regard. Under the erstwhile Evidence Act of 2011, the admissibility of computer-generated evidence was introduced under Section 84. The 2011 Act also defined a document as including any device by means of which information is recorded, stored,

or retrievable, including computer output (Section 258). However, more was needed to improve the admissibility of evidence, particularly electronically generated evidence, as contained in the Evidence Act of 2011. Hence, the Evidence (Amendment) Act of 2023 introduced novel digital and electronic execution of documents and the admissibility of storage mediums as evidence.

Under the new Nigerian Evidence (Amendment Act) of 2023, an electronic record is defined to include "data, record or data generated image or sound stored, received, or sent in an electronic form or micro film" (Section 84). The word "electronic record" has been specifically inserted after the word "document" throughout the entire section 84, which deals with computer-generated evidence in the Act. This implies that documents or electronic records satisfy the laid down conditions of the Act. Specifically, Section 10 of the Evidence (Amendment Act) 2023 provides that electronic records printed on paper, stored and recorded or copied in optical or magnetic media or cloud computing database produced by a computer are now admissible in any judicial proceeding before Nigeria courts without further proof or production of the original, if the conditions enumerated in the Act are met. This provision was not contained under the previous 2011 Evidence Act. The 2023 Evidence Act introduced the use of digital signatures in legal documents. Section 10 of the new Act went further to define a digital signature as one that is generated electronically and attached to a document that is electronically transmitted in order to verify the contents or authenticity of the document and the identity of the sender. In the same vein, the Act now recognizes the use of digital signatures in court documents or legal processes. It is important to note that one should authenticate a digital signature. In line with the requirement of the law that for a document to be admissible in evidence, same must be duly executed or authenticated, the Act has provided for the authentication of electronic records through the use of digital signatures in such manner or by such technique as may be stipulated by the Act or such other technique as the Court may consider reliable. The Conditions for reliability as provided by the Act include:

a) The data for creating the signature or the authentication data, within the context of usage, can only be linked to the signatory or authenticator and none other;

b) Where an alteration is made to the digital signature after affixing it to the electronic record for authentication, such alteration must be detectable;

c) Where the information contained in the electronic record is altered after the same has been authenticated by the digital signature, such alteration must be detectable, and such other conditions as may be prescribed by law.

Additionally, for a duly authenticated electronic record to be admissible, a digital signature alleged to have been affixed by a person must be proven to belong to such person. This, however, does not apply to a secure digital signature, and a digital signature will be deemed to be secure if:

a) The creation date of the signature was under the exclusive control of the signatory alone.

b) The same was stored or affixed exclusively as may be prescribed.

Tendering a digital certificate issued by a trusted Certificate Authority (CA). The CA will verify the person's identity and issue a certificate that confirms the authenticity of one's digital signature. It is glaring that this is not explicit or explanatory enough. This is not a reliable digital signature authentication technique.

The advantages of digital and electronic signatures cannot be overemphasized. Digital and electronic signatures provide a higher level of security. They use encryption technology to ascertain the integrity and authenticity of the signed document. This will forestall forgery, tampering, and alterations. The electronic signature also facilitates speedy transactions as there will be no need for physical paperwork printing or mailing. Court processes, land transaction documentation, and contractual documents can also be signed by parties electronically and transmitted in the same way. This will facilitate faster court processes, save time spent on perfecting agreements, and ultimately increase efficiency. With digital and electronic signatures, parties to a transaction can afford to sign or access the documents from anywhere at any time. There would be no need for parties to hold physical meetings. Hence, this will facilitate cross-border and international transactions. The digital and electronic signatures will create an enabling environment for the audit trail. It easily provides a comprehensive record of when, who, and how a document was signed will be on record. This will promote accountability and will be handy in the resolution of any discrepancies that may arise in the future (Ayojimi, 2024).

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

This was enacted by the National Assembly to ensure an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Cybercrime Act was signed into law in 2015. The Act contains 59 sections, is divided into 8 parts, and it has two (2) schedules. The Act applies throughout the Federal Republic of Nigeria. The implication is that any other law made with respect to cybercrime by a State House of Assembly is void or inactive, as the case may be. It is worth noting that cybercrimes may take different forms, but the impact on electronic transactions is enormous, be it electronic commerce, electronic governance, electronic education, or any other form of electronic transactions. Hence, several provisions of the Cybercrimes Act relate to electronic transactions.

Under the Act, the term "cybercrime" was not defined at all. This leaves the meaning and scope of what constitutes cybercrime in Nigeria to speculation. Also, under Section 48 of the Act, a law enforcement officer may apply *ex-parte* to a judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence related to a crime investigation. The judge is to issue a warrant authorizing law enforcement officer to enter and search any premises or place if within those premises, place, or conveyance an offence under the Act is being committed, or there is evidence of the commission of an offence under the Act; or there is an urgent need to prevent the commission of an offence under Act.

Under Section 6(1) of the Act, it is an offence for any person without authori-

zation to intentionally access, in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security. It is an offence under the Act to intentionally obtain computer data, and secure access to any program, commercial or industrial secrets, or classified information (Section 6(2)). It is an offence under the Act to unlawfully intercept data or to either directly or indirectly modify or cause the modification of any data held in any computer system or network by way of alteration, erasure, removal, suppression, or prevention of the normal operation of the computer system or network (Section 16(1). Under the Cybercrime Act, it is an offence to use any device for the purpose of avoiding detection or otherwise preventing identification or attribution with any of these acts or omissions (Section 6(3)).

The Act under Section 7 made it mandatory for all operators of cybercafes to register with the Computer Professional Registration Council in addition to being registered as a business name with the Corporate Affairs Commission. The Act also mandated all cybercafe operators to maintain a register of users through sign-in personnel whenever needed. Section 7 subsection 2 also provides that any person who perpetrates electronic or online fraud using a cybercafe commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of N342,000,000.00 or both. The question is whether this can be implemented as most cybercafes in Nigeria are not even registered as a business name with the Corporate Affairs Commission, not to mention registering with the Computer Professional Registration Council. It is submitted that this will amount to a clog in the wheel, particularly in the enforcement area. The inclusion of CPRC in the enforcement realm will amount to the decentralization of the enforcement framework. It is submitted that it will be most appropriate to have a single enforcement institution to fight against the menace of cybercrime in Nigeria. (Snail ka Mtuze & Nwafor, 2022)

Another striking provision of the Cybercrimes Act is that it is an offence for any person to destroy or abort any electronic mails or processes through which money or any valuable information is being conveyed (Section 9). The Act is silent on what the term "valuable information" means. This makes room for guessing and speculation. There is a duty imposed on financial institutions to safeguard their customer's sensitive information.

Under Section 17(1) 9 (Cybercrime Act, 2015), electronic signature with regard to purchases of goods and services and any other transactions shall be binding. No transaction would be denied enforceability simply because the transaction was electronically signed. Whenever the genuineness or otherwise of electronic signatures is in question, the burden of proof that the signature does not belong to the purported originator of such electronic signature shall be on the contender (Section 17(1) a).

The Act also provided that any person who with the intent to defraud or misrepresent, forges through electronic devices, another person's signature or the mandate of a company commits an offence. The said offence is punishable with impris-

onment for a term of not more than seven years or a fine of not more than N10 million naira or both fine and imprisonment (Section 17(1) c).

However, under the Act, there are exemptions to transactions that can be electronically signed, for example, death and birth certificates, wills, family law matters. Under Section 37 of the Act, financial institutions are mandated to verify the identity of their customers carrying out electronic financial transactions and execute the documentation of customers preceding the execution of customers' electronic transfer, payment, debit and issuance orders (Section 37 (1) a&b). This section ensures that financial institutions uphold an effective mechanism against financial malpractices in banking transactions. It ushers in a new dawn in electronic commercial transactions in the financial world due to the duty of care imposed on financial institutions. Additionally, Section 38 of the Act mandated service providers to keep all traffic and subscriber information as may be prescribed by the relevant authorities responsible for regulating communication services in Nigeria for 2 years. Service providers are required to retain content and non-content information and make such available to an authorized law enforcement officer. The Act mandates that any data retained shall only be used for legitimate purposes as may be provided for under the Act, any other legislation, regulation, or by order of a court of competent jurisdiction. Appropriate measures to safeguard the confidentiality of the data retained must be taken, and the individual's right to privacy under the Nigerian Constitution must be respected.

3) Nigeria Data Protection Act 2023

The Federal Government of Nigeria in an effort to regulate personal data in Nigeria, enacted the Nigeria Data Protection Act 2023, also known as the (NDPA). This comes after the Nigeria Data Protection Regulation issued by the National Information Technology Development Agency (NITDA) in 2019. This Act replaced the erstwhile Nigerian Data Protection Regulations (NDPR) 2019 and the Nigerian Data Protection Regulations Implementation Framework 2019 which was issued under the National Information Technology Development Agency (NITDA). This present Act of 2023 established the Nigeria Data Protection Commission.

The NDPA basically applies to the processing of personal data by a data processor, whether automated or not, that belongs to data subjects in Nigeria. It is pertinent to note that it is immaterial whether the data controller or data processor is not operating in Nigeria. However, as long as the data subjects are domiciled in Nigeria, the NDPA must surely apply. Where Nigerian citizens are residing outside Nigeria, the NDPA will not protect them. It is worth noting that there are circumstances under the Act where the NDPA will not apply to a data controller or data processor.

The exceptions include:

a) the prevention, investigation, detection, prosecution, or adjudication of a criminal offense or to execute a criminal penalty in accordance with any applicable law;

b) to prevent or control a national public health emergency;

c) as is necessary for national security;

d) in respect of publication in the public interest, for journalism, educational, artistic, and literary purposes to the extent that such obligations and rights are incompatible with such purposes;

e) necessary to establish, exercise, or defend legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

It is pertinent to state that all digital businesses and platforms are under obligation to abide by the legal and regulatory requirements under the Act or face the penalty contained therein.

5. Challenges Associated with the Enforcement of Digital Transaction Laws towards Achievement of SDGs in Nigeria

Firstly, it is paramount to note that in Nigeria, we have a limited number of legislations with regard to the regulation of electronic transactions as well as the proliferation of cybercrimes. In addition, the existing legislation did not make any provisions or adequate consumer protections with respect to regulating tech giant's digital payments and smartphone wallet services in Nigeria. (Lubis & Handayani, 2022)

Secondly, our enforcement mechanism is very poor in Nigeria. Government bodies that are charged with compliance with the statutory provisions of the law are inefficient. Most of the enforcement agencies are bedeviled by corruption and corrupt practices.

Defaulters to the provisions of our extant legislation must be punished adequately so as to deter would-be offenders from venturing into the same. Non-compliance should be taken seriously.

Members of the public should be sensitized to their rights under various legislations. There should be a massive awareness program by the government, government agencies, non-profit organizations, and a host of civil society groups on the provisions of the novel laws that are being made in Nigeria. Creation of awareness on how cybercriminals operate will, in no small measure, reduce the exposure of unsuspecting members of the public to falling victim to cybercrimes.

Additionally, data controllers and data processors are to ensure strict compliance with the letters and intendment of the laws, which will exonerate them from liabilities.

6. Conclusion

Cybersecurity is a global issue that demands international cooperation and synergy. It is imperative to note that efforts should be targeted at strengthening global frameworks and treaties on cybersecurity, promoting cross-border collaboration in cyber threat intelligence, and establishing international norms and standards for cybersecurity that support the SDGs. In addition, while the analysis has cen-

tered on the cybersecurity threats that pose risks to achieving the SDGs, the dual nature of cybersecurity as both a challenge and an opportunity for sustainable development is also appreciated. The most obvious results of cybersecurity incidents are financial losses; however, cyber incidents can also result in costly recovery or remediation and, in certain cases, litigation; serious harm to consumers' privacy, resulting in potential fines imposed on the basis of regulations, such as the General Data Protection Regulation (GDPR), which can amount to 20 million euros or 4% percent of an organization's worldwide turnover; impaired organizational operational integrity, infringement of intellectual property rights, and bad reputation. It is glaring that the digital era has posed a lot of legal challenges as well as towards achieving the sustainable development goals in Nigeria. It has also exposed the lacuna in our present laws. As the years unfold, the scope of cybercrime is growing rapidly. As countries attempt to beef up and proactively secure their digital payment system laws, the threat of cyber fraud continues, hence the urgent need for novel changes in our laws. An increase in cybercrime is a global menace, and it is double jeopardy to Nigeria's businesses and its citizens. There is an urgent need to enhance the growth genuineness and sustainability of digital transactions through effective and adequate legal frameworks.

Even though the Nigerian government has recently taken steps to bridge the gap in our legal framework with respect to digital transaction processes and protect its citizens against fraud, much still needs to be done. At the international level, electronic or digital transactions have gained so much prominence that it has specific laws regulating them. For example, the United States has the Electronic Signatures in Global and National Commercial Act 2000 and the Uniform Electronic Transactions Act at the State level. Also, in the United Kingdom, they have the United Kingdom's Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. In South Africa, there is the Electronic Communications and Transactions Act 2002.

7. Recommendations

Cyber security and cyber warfare are a continuum. The digital space is no longer a lawless frontier; rather, nations of the world are now alert to making laws to ensure that the cyberspace is safe. It is pertinent to state that digital transactions are the foundation of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies.

In Nigeria, there is an urgent need to have a legal framework dedicated solely to the regulation of electronic or digital transactions as is obtainable in some other jurisdictions. There is no law in Nigeria that is dedicated to this urgent, precarious situation; this has, to a great extent, hindered the ease of doing business in Nigeria. There is also the need to consider the recognition of electronic identification, authentication, and trust services in the African region that would recognize the legal validity of digital signatures and stamps as well as their admissibility as evidence across member states. This will enhance trade relations across the continent.

The government of Nigeria needs to create and or establish a digital or electronic systems regulator. They should be charged with statutory duties to promote innovation and ensure that digital/electronic transactions are operated and conducted in a way that promotes the interests of businesses and consumers. Individuals should be able to express and engage freely on the internet, having the confidence that their personal data will also be protected.

The Nigerian government should organize educational campaigns to educate, sensitize, and inform the public about the benefits and dangers of electronic or digital payment systems. People should be taught how to seal deals electronically, how to use digital payment methods, and how to detect cyber-fraudsters.

On a global scale, there is an urgent need for countries on international and regional levels to drive greater interoperability and inclusivity with a view to coherent and efficient regulatory reforms for digital payment systems.

The Nigerian judiciary should embrace the use of electronic evidence as a means of administering criminal justice. Judges, legal practitioners, and public prosecutors should be trained, be proactive, and embrace the use of digital forensic tools. Thus, digital forensic tools are applications and devices that are geared toward facilitating the investigation and analysis of digital evidence. This will improve the efficiency and effectiveness of our justice delivery system in Nigeria.

Conclusively, the world must together take note of the inherent challenges of criminals in cyberspace and work towards harmonized national and international policies so as to synergize the war against cybercrimes and a safe cyberspace for digital transactions.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Aguboshim, F. C., Obiokafor, I. N., & Emenike, A. O. (2023). Sustainable Data Governance in the Era of Global Data Security Challenges in Nigeria: A Narrative Review. *World Journal of Advanced Research and Reviews, 17,* 378-385. https://doi.org/10.30574/wjarr.2023.17.2.0154

AU Worldwide (2022). *Prime-Time for Real Time* (3rd ed.). NASDAQ: ACIIN.

Ayojimi, M. (2024). *The Evidence Act of 2023: A Remarkable Advancement in Nigeria's Jurisprudence*. https://lawpavilion.com/blog/the-evidence-act-of-2023-a-remarkable-advancement-in-nigerias-jurisprudence/

Businessday Newspaper Nigeria (2022, November 18). Nigeria Recorded a 174% Increase in Cybercrimes in Six Months. Business Day. https://www.businessday.ng

Cybercrime (Prohibition, Prevention, Etc) Act 2015.

Digital Payments in Nigeria. https://www.statistic.com

Hoar, S. B. (2001). Identity Theft: The Crime of the New Millennium. *Oregon Law Review, 80,* 1423-1448.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Foren-*

sics: An Introduction. Routledge.

Lubis, M., & Handayani, D. O. D. (2022). The Relationship of Personal Data Protection towards Internet Addiction: Cyber Crimes, Pornography and Reduced Physical Activity. *Procedia Computer Science, 197,* 151-161. https://doi.org/10.1016/j.procs.2021.12.129

Organization for Economic Corporation and Development (OECD) (1997). *Report on Electronic Commerce: Opportunities and Challenges for Government* (p. 20).

Queen Troanusi, over 2,800 Persons Convicted of Cybercrime in 2022—EFCC. https://www.premiumtimesng.com

Rathna, G., Mohan, S., & Jayalakshmi, J. S. (2023). *Cybercrime and Digital Payments in India: A Comprehensive Analysis, India*.

Snail Ka Mtuze, S., & Nwafor, I. (2022). Dr. Ifeoma Nwafor: Cybercrime and the Law: Issues and Developments in Nigeria. (2022) CLDS Publishing. PP. 1-285. *International Cybersecurity Law Review, 4,* 253-254. https://doi.org/10.1365/s43439-023-00080-3

World Economic Forum (2018). World Economic Forum Annual Meeting 2018' Creating a Shared Future in a Fractured World, Davos_Klosters, Switzerland 20 26 January 2018. https://www.weforum.org