A REVIEW OF THE LAW DEALING WITH CYBER CRIMES IN NIGERIA: A CRITIQUE OF THE CURRENT LAW AND HIGHLIGHT OF YAWNING GAPS

By

Badariyyah Rabi'u Abubbakar•

ABSTRACT

In Nigeria the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 had been the principal legislation in suppressing cybercrimes offences. This Act was critised for vague provisions, misuse against journalists and weak enforcement mechanisms. The Amendment Act, Cybercrimes (Prohibition, Prevention, Etc.) Act 2024 (as Amended) updates the former Act to clarify drafting gaps, broaden certain offences, introduce new compliance and reporting duties, and create funding and institutional measures aimed at strengthening Nigeria's cyber-security architecture. However, notwithstanding the progress of the Amendment Act, it introduces fresh tensions and challenges between security, economy and civil liberty. Among the challenges are: unresolved issues around legal ambiguity e.g, vague terms/provision of some sections, Another challenge is the controversy of the provision of section 44 of 0.5% cyber-security levy on specific electronic transactions to finance the National Cyber-security Fund. The aim of the paper is to critically examine the Amendment Act 2024, highlights its reforms, controversies, broader implications of law, policy and rights. This paper used doctrinal methodology to buttress issues at hand. The paper found that section 24 of the Act on cyberstalking remains vague leaving space for prosecutorial abuse against journalists, activists, or online critics. The paper recommended that the Nigerian legislature should take a rapid step to re-amend the Cybercrimes (Prevention, Prohibition Etc.) Act 2024 to clearly define the inception for criminal liability, restricting it to speech that directly incites violence/grievous harm in accordance with the constitutional and international free expression standards. The paper concluded that the Act still faces criticisms and concerns remains about, enforcement challenges, jurisdictional issues, potential misuses, vague definition, and need for review.

• Lecturer, Faculty of Law, Northwest University Kano, Kano State. talk2riyyah@gmail.com +234 8030412836

1.0 Introduction

The main objective of carrying out the cybercrimes activities is financial gain, which is achieved through the use of unauthorised access to bank account of government, individuals and businesses. The dynamic nature of cybercrime, characterised by its continuous evolution and the sophisticated methods employed by perpetrators, poses significant challenges to the global legal framework. This complexity is further compounded by the diversity in the legal landscapes of different jurisdictions, each with its own set of laws, enforcement strategies, and challenges. The legal frameworks governing cybercrime vary widely across regions, reflecting differences in legislative priorities, technological advancements, and the perceived threat level of cyber activities.[1]

Most countries have enacted their cyber laws for the prevention and control of cybercrime.[2] It is paramount to note that the Nigerian National Assembly has enacted legislation to curb and eradicate crimes associated or related to the use of computer and information technology, offences are created and severe punishment prescribed for those offences. Despite the enactment and commendable provisions of this Act, to eliminate cybercrimes, cybercrimes continue on the increase. On the other hand, several ambiguities, inconsistencies and factors in relation to its implementation of which have been described as violation of constitutionally guaranteed rights necessitated the legislator's move to review and amend the principal Act 2015. Currently, the Cybercrimes [Prohibition, Prevention, Etc.] Act, 2024 remains the comprehensive legislation for combatting cybercrime in Nigeria. The Act provided for a legal, institutional and procedural framework for the detection, prevention and prosecution of cybercrimes in Nigeria.

The Cybercrimes [Prohibition, Prevention, Etc.] Act 2024 aims principally at clearing ambiguities in the principal Act which previously hindered their effective implementation; and to widen the scope of applicability of the provisions of the Act. New sections were inserted after some sections of Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015. This paper reviews and provides an analysis of the Nigerian legal regime designed at suppressing cybercrimes. Also, the paper reviews the legislation, analyses the offences under it, further examine and analyse the key provisions and innovations introduced by the amended Act Cybercrimes (Prohibition, Prevention, Etc.) Act, (as

[1] Enver Buçaj and Kenan Idrizaj, 'The need for cybercrime regulation on a global scale by the international law and cyber convention', *Review Article* (2025) <http://www.malque.pub> accessed 7 May 2025.
[2] ibid.

Amended) 2024, exploring its impact on both Nigerians and the cyberspace landscape upon implementation. The Prohibition of cybercrimes can be inferred from some of provision of the below laws while some are directly prohibiting cybercrimes.

1.1 Legal Regime/Mechanism for Combating Cybercrime

The system of laws and rules that govern cybercrimes in Nigeria comprise of various regime, each with its own unique and distinct principles, characteristics and applications. This paper is not going cover all the Nigerian legal regime in relation to criminal justice, but will explore the concept of the following legal regimes, examining their significance as well as the challenges they encounter in promoting justice, predictability and stability these include: The constitution of the federal republic of Nigeria,[3] the Nigerian Criminal Code Act,[4] the Evidence Act:[5] Nigerian Communication Commission Act,[6] Economic and Financial Crimes Commission Act,[7] Advance Fee Fraud and other Related Offences Act,[8] Terrorism (Prevention and Prohibition) Act,[9] Administration of Criminal Justice Act,[10] and Nigeria Data Protection Act,[11]

This paper hold the view that the above legislation has not elaborate in enumerating acts and activities that constitute cybercrimes. E.g, Terrorism (Prevention and Prohibition) Act has not explicitly defined cyberterrorism. Thus, in view of this paper that the Act is not specifically made as handy tool in prosecuting cybercrimes dealing with cyber terrorism committed online or by computer network. This paper is of the opinion that though, cybercrimes falls within the realm of crimes CAJA has not specifically addresses offences in relation to cybercrimes. Thus, CAJA may not be satisfactory on its own to effectively prosecute cybercrimes, thereby creating a gap for enforcement. NDPA does not cover all aspect of cybercrime which are addressed in cybercrimes Act. From the foregoing discussions so far conversed, it is obvious that all the above legislation

[3] The 1999 Constitution of the Federal Republic of Nigeria (as Amended). The Constitution of the Federal Republic of Nigeria, has been the principal legislations for criminal justice in Nigeria. The constitution as a grundnorm enshrines the right to privacy and freedom of expression as a fundamental rights. See sections: 22, 37, 39 and 45.
[4] The Criminal Code Act Cap C 38 Laws of the Federation of Nigeria, 2004. The specific provision relating to cybercrime in the Criminal Code is section 419 which deals with obtaining property by false pretenses or cheating.
[5] Evidence (Amendment) Act 2023. See section 84 of the Act.
[6] The Nigerian Communication Commission Act no.19 2003, see Section 146.
[7] The Economic and Financial Crimes Commission (Establishment) Act, 2004. It deals with financial crimes and cyber related crimes.
[8] The Advance Fee Fraud and other Related Offences Act, 2006, see section 2.
[9] The Terrorism (Prevention and Prohibition) Act, (As Amended) 2022.
[10] Administration of Criminal Justice Act, (ACJA) 2015. See Section 1(1).
[11] Nigeria Data Protection Act, 2023. See Section 4.

have proven ineffective in curbing cybercrime as it is increasing. In a bid to put in place a stronger legal framework to curb cybercrime, the Government put forward a revision of the existing cybercrime legislation.[12]

1.2 Cybercrimes [Prohibition, Prevention, Etc.] Act, (As Amended) 2024.[13]

The epidemic of cybercrime in the world and Nigeria, in particular, is at an alarming high thus, there must be in place a legal mechanism to combat cybercrime. Hence the enactment of Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024. Key provisions in the amended act include: Implementation on the Cyber-security Levy;[14] Establishment of Computer Emergency Response Team (CERT) and Security Operational Centre (SOC);[15] Reporting of cyber threat;[16] Inclusion of the requirement of National Identification number;[17] Protection of specific traffic data and subscriber information[18] and Manipulation of ATM/POS terminals.[19]

While the Act has improved Nigeria's cybercrimes response, [20] notwithstanding the numerous improvement to the Nigerian legal system, some provisions in the Act have been criticized for having been used to stifle critical writing, silence opposition views, roll back digital rights, ambiguously worded[21] restriction of right to freedom of expression, potential abuse by government authority, vague and generic provisions, etc.[22] are seen as the shortcoming of the Act.[23]

---

[12] Abiodun Adebanjo and Gloria Chigbu and Christopher M Osazuwa, 'Effect of Data Protection Frameworks against Cybercrimes on Cyber Security in Nigeria' *The American Journal Of Political Science Law And Criminology* (2024) 6(9) <http://AA Dop. G Chigbu, CM Osazuwa - ... Journal of Politrical Science Law and ..., 2024 - inlibrary.uz> accessed 7 May 2025.
[13] Cybercrimes [Prohibition, Prevention, Etc.] Act, (as Amended) 2024.
[14] ibid. Amended section 11.
[15] ibid. Amended section 10.
[16] ibid. Amended section 3.
[17] ibid. Amended section 8.
[18] ibid. Amended section 9.
[19] ibid. Amended section 7.
[20] Onatuyeh E. A. and other, 'Cybersecurity and Business Survival in Nigeria: Building Customer's Trust' *African Journal of Applied Research* (2025) 11(1) <http://EA Onatuye, D Oghorodi, EA Okpako... - African Journal of ..., 2025 - ajaronline.com> accessed 7/5/2025.
[21] Godswill Owoche Antai and others, 'Press Freedom and National Security: The Place of Human Rights in Nigeria's Cybercrime Laws' *NIU Journal of Social Sciences* (2025) 11(1) <http://GO Antai, OO O bisesan, ME Umo, H Ismaila… - NIU Journal of Social …, 2025 - ijhumas.com> accessed 3 May 2025.
[22] EFG Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' [2016] 6(1) Journal of International and Information System.
[23] Antai (n 21).

1.3 Discussions/Critiques of Selected Sections and Expressions

The paper tempts to review some sections and key changes made by the amendment Act that are pertinent to this research which comprises the following:

1.3.1 Designation of Certain Computer Systems or Networks as Critical Information Infrastructure (Section 3).

The President may on the recommendation of the National Security Adviser, by order published in the Federal Gazette, designate certain computer systems, and or networks whether physical or virtual and or the computer programs, computer data and / or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating on the security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.[24] Such critical National Infrastructure offence is punishable under section 5.[25] The critical Infrastructure has been interpreted by the Act to means, systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national security, national public health and safety of the country.[26]

It is argued that, the implication of this provision is that for a matter to be deemed as a Critical National Information Infrastructure, such matter shall be so vital to the circumstances and matters stated in the section. The phrase "so vital" is a subjective clause and this is a very dangerous situation especially as the Act makes no provision for checks and balances from the Executive. The President may designate a matter not as vital as so vital or may overlook a matter so vital without designating same as such.[27]

[24] Cybercrimes Amended Act 2024 (n 13) section 3.
[25] ibid. Section 5(1) A person who with intent commits any offence against any critical national information infrastructure under section 3 is liable to 10 years imprisonment without option of fine. (2) Where the offence committed under subsection 1 results in grievous bodily harm to any one, the offender is liable to 15 years imprisonment without option of fine. 3) Where the offence committed under subsection 1 results in the death of a person, the offender is liable to life imprisonment.
[26] ibid. Section 58.
[27] Aisha Oluwakemi Balogun, 'The Legal Battle against Cybercrime in Nigeria: An Assessment of Current Laws' *Public Policy and Administrative Studies Journal* (2024) 12(4) <http://AO Balogun - Public Policy and Administration Studies Journal, 2024 - keithpub.com> accessed 7 May 2025.

1.3.2. Unlawful Access to Computer (Section 6).

Under Section 6 of the Act, it is an offence for any person without authorization 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.[28] It is an offence under the Act to intentionally obtain computer data, secure access to any program, commercial or industrial secrets or classified information.[29] 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. Under the Cybercrime Act, it is an offence to use any device for the purpose of avoiding detection or otherwise prevent identification or attribution with any of these acts or omission.[30]

The Act in this section raises the issue of intent to commit a crime. Intention to commit crime is a fact very difficult to prove. The position of the Evidence Act on facts bearing on question whether an act was accidental or intentional[31] could not be very useful in this circumstance considering the type of crime which this Act refers to. A smart cybercriminal may escape liability by showing that the crime he is being prosecuted for is not intended by him. Also the law enforcement agencies may not have the wherewithal to categorically pin the accused to the crime as it may be difficult to prove intention in cyber activities wherein punching a button may lead to various results. Going by the above scenario, it is argued that it would have been better if strict liability is prescribed for such offences.[32]

1.3.3. Mandate of Cybercafé Registration (Section 7).

The Act under Section 7 made it mandatory for all operators of cybercafés to register with Computer Professional Registration Council in addition to being registered as a business name with the Corporate Affairs Commission.[33] The Act also mandated all cybercafé operators to maintain a register of users through sign-in personnel whenever needed.[34] It is also provided that any person who perpetrates electronic or online fraud using a cybercafé commits an offence and

[28] Cybercrimes Amended Act 2024 section 6(1).
[29] ibid. Section 6(2).
[30] ibid. Section 6(3).
[31] ibid. Section 7.
[32] Evidence Act 2023 (n 5) section 12.
[33] Cybercrimes Amended Act 2024 (n 13) section 7.
[34] ibid. Section 7(b).

is liable on conviction to imprisonment for a term of 3 years or a fine of N342, 000,000.00 or both.[35]

The question is whether the above can be implemented as most cybercafés in Nigeria as not even registered as a business name with Corporate Affairs Commission talk less of registering with Computer Professional Registration Council. It is submitted that this will amount to a clog in the wheel particularly in the area of enforcement. The inclusion of Computer Professional Registration Council (CPRC) in the enforcement realm will amount to decentralization of the enforcement framework. It has been a view that it will be more appropriate to have a single enforcement institution to fight against the menace of cybercrime in Nigeria.[36]

Under the Act, connivance between a cyber-criminal and an owner of a cyber café to perpetrate an electronic fraud or online fraud using a cyber café is an offence,[37] and the burden of proving such connivance rests on the prosecutor.[38] Some writers are of the opinion that this burden of proof on the prosecution is an onerous task which may vitiate the smooth working of the core aim of this Act. There are instances where the prosecution is not computer literate. Even when they have some knowledge of the computer, they may not possess the enabling forensic knowledge to tackle the crime. In some other cases, the judge before whom the matter may be brought may not be literate on the workings of computer systems and the network to satisfy himself of connivance even when the prosecution is striving to prove its case.[39]

For instance, Judges and lawyers in Nigeria may lack sufficient training in the nuances of AI and digital evidence, leading to challenges in adjudicating cases involving AI-driven cybercrime. For example, interpreting data from AI tools or understanding algorithmic biases may be beyond the technical understanding of many in the legal profession.[40] This situation may create a soft landing

[35] ibid. Section 7(2).
[36] Ngozi Chisom Uzoka and Nneka Obiamaka Umejiaku, *Cybercrime and Digital Transactions Law in Nigeria: A Review* (Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024) <http://NC Uzoka, NO Umejiaku - researchgate.net> accessed 7 May 2025.
[37] Cybercrimes Amended Act 2024 (n 13) section 7(3).
[38] ibid. section 7(4).
[39] Balogun (n 27).
[40] E. O. C. Obidimma and Richard Onyekachi Ishiguzo, 'Artificial Intelligence and Cybercrime Investigation in Nigeria: Addressing the Legal and Technical Skills Gaps' *African Journal of Criminal Law and Jurisprudence (AFJCLJ)* (2023) 8 <http://EOC OBIDIMMA, RO ISHIGUZO - …, Journal of Criminal Law …, 2023 - ezenwaohaetorc.org > accessed 7 May 2025.

for the cyber café owners to escape liability. The liability in this instance ought to be strict so as to deter intending offenders.[41]

1.3.4. System Interference and Intercepting of Electronic Messages, emails and Electronic Money Transfers (Section 8 and 9)

A person commit an offence where without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serous hindering of functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with computer system, which prevent the computer system or any part thereof, from functioning in accordance with its intended purpose.[42] 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.[43]

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 safely guard their customer's sensitive information.[44] In addition to this, going by provision of sections 8 and 9, both sections do not prevent the creation and distribution of computer viruses among people.

1.3.5. Theft of Electronic Devices (Section 15).

It has been criticized that some offences cover the broad spectrum of computer-dependent and computer-enabled crimes whilst others, such as section 15 which criminalises the theft of electronic devices, cannot possibly be classifiable as cybercrime. This offence in particular is curious.[45] Section 15 criminalises (a) the act of stealing a financial institutions or public infrastructure terminal and (b) stealing an Automated Teller Machine (ATM).[46] Neither of these acts are computer enabled nor computer dependent and therefore cannot be classified as

[41] Balogun (n 27).
[42] Cybercrimes Amended Act (n 13) Section 8.
[43] ibid. Section 9.
[44] Obidimma and Ishiguzo (n 40).
[45] Sagwadi Mabunda and Roland Akindele, 'On Legislating Cybercrime: Nigerian, South African, and United Kingdom Perspectives', International Information Management Association (IIMA) Conference Proceedings 2024 <http://scholarworks.libcsusb.edu> accessed 7 May 2025.
[46] Cybercrimes Amended Act (n 13) Section 15(1) and (2).

cybercrimes by any stretch of the imagination. They can only be defined as an ordinary act of theft and could have been dealt with under the existing laws.

1.3.6. Extended Scope on the use of Electronic Signature (Section 17)

For the purpose of this section, "signature", with it grammatical variation and cognate expressions, shall, with references to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.[47] The Cybercrimes 2015 Act excluded some contractual transactions and documents from the categories of documents that can be validated by electronic signature. This includes death certificate, birth certificate, wills etc.[48]

The Amended Act retains this provision generally but allows for the use of electronic signatures in respect of such transactions and documents when they are legally verified in certified true copies.[49] This means that these transactions and documents can be validly completed with electronic signatures if the documents or documentation used for the transaction are in fact legally verified in certified true copies by the issuing entity. Thus, there is an added layer of responsibility on concerned parties to ensure that the documents are first verified before such parties can resort to the use of electronic signatures.[50]

However, the practical implementation of this provision is unclear. It is so said because, it is unclear how a party who intends to execute a document electronically should first certify the document that is yet to emanate from him. For example, the chairman of the National Population Commission cannot certify a birth certificate that has not yet been issued. It seems the intention of the Amended Act may be to allow for certification after the document has been executed. It is opined that the provision be reworded to either permit the use of electronic signatures without additional requirements or specify that the certification of electronic signatures can occur after the document's execution in certain circumstances.[51]

[47] Yatindra Singh, *Cyber Laws* (5th edition Universal Law Publishing Co. Pvt. Ltd, 2012).
[48] Cybercrimes [Prohibition, Prevention, Etc.] Act, 2015, Section 17.
[49] Cybercrimes Amended Act 2024 (n 13) Section 17, Amendment section 2.
[50] ibid. Section 17(4).
[51] Emmanuel Gbahabo and Lawal Kazeem and Christiana Ufomba, 'The Cyber Crimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024: A Paradigm Shift for Individuals and Businesses?' *TEMPLARS ThoughtLab* (2024) <http://www.templars-law.com> accessed 7 May 2025.

1.3.7. Exception to Financial Institutions, Posting and Authorized Options (Section 19).

Sometimes, the burden of proof appears to rest on the computers and systems through which these acts of cybercrime are committed since the bank has done all that is required of it to ensure that occurrence of fraud is ruled out. This could seem so in the instance of an Automated Teller Machine (ATM) and Point of Service Machines (POS) which are operated and accessed at any time of the day including weekends and public holidays within and outside the bank, in the absence of the affected bank and its staff as the case may be. One may conclude that the bank should not be held responsible for any crime committed in the process of using these computer systems by a customer especially when the bank or its staff is not present and the bank management has placed all counter fraud measures in place.[52]

The line of argument may appear credible on the face of it. However, it is worthy of note that a machine and or a computer is a programmed system which displays or functions according to an instruction or command. Again, in other civilized countries where banking systems are computerized, banking programmes are frequently checked to detect interference or attack and when such is detected, it is blocked and the existing programme changed immediately. Also, computers in such civilized nations are programmed to detect foreign bodies and interference. This is to ensure that perpetrators of cybercrime do not have their way into customers' accounts and if for any reason it happens, then it is detected on time before greater harm is done.[53]

Allowing the banks to escape liability once it is proven that all counter fraud measures are put in place without more could be an onerous one on the customer who may not have the requisite technological expertise or the financial power to engage an expert to prove that the financial institution is actually negligent even when it is clear that it is negligent. Some writers further opined that the Act would be better if there is strict liability on the part of the financial institutions since they are the custodians of this leaked information. They should be made to prove that they are actually not liable.[54]

[52] Balogun (n 27).
[53] ibid.
[54] ibid.

1.3.8. Extension of Scope for Identity, Theft and Impersonation (Section 22).

Under the 2015 Act, any employee of a financial institution who uses his/her special knowledge to commit identity theft against his/her employer, staff, service providers, or consultants with the intent to defraud is guilty of an offense.[55] Identity theft and impersonation contemplates unlawfully obtaining and using another person's personal or financial information with the intent to deceive or defraud or assume another person's identity, typically to access resources, obtain credit, or conduct unauthorized transactions in the victim's name.[56]

Under the 2015 Act, staff members of companies other, than financial institutions, could not be tried for identity theft and impersonation. This created an obvious loophole that could be exploited by unscrupulous employees of companies other than financial institutions, to defraud or generally harm unsuspecting members of the public.[57] To correct this anomaly, the Amended Act extended the scope of service providers whose staff member could be tried for identity theft and impersonation to cover persons engaged in the services of public or private organizations.[58]

1.3.9. Protection of Child Pornography Abuse (Section 23).

Technology allows children to connect with their family, friends and others in ways that enrich their relationships, especially when using video chat and other real time interactions, it helps children become independent learners more quickly, once the learn how to access digital information sources safely, they are able to explore the topics that interest them on their own. It also teaches digital literacy skills that children will need for their future success in school. And as well as the Negative effects of digital technology on children like exposure to harmful online content and sexual exploitation, cyber bullying, low self-esteem and increased anxiety, another negative effect is the physical harm TV and Phone Screens does to eyes of the children.[59]

---

[55] Cybercrimes Act 2015 (n 48) Section 22(1).
[56] Temitope Lawal, Kunle Ola and Helen Chuma-Okoro, 'Towards the recognition of internet access as a human right in Nigeria: a theoretical and legal perspective' *International Review of Law, Computers & Technology* (2025) <http://T Lawal, K Ola, H Chuma-Okor - International Review of Law …, 2025 - Taylor & Francis> accessed 7 May 2025.
[57] ibid.
[58] Cybercrimes Amendment Act 2024 (n 13) section 22, Amendment Section 4.
[59] Sikkam Ibrahim Suleiman, 'Policy Regulations for the Use of Digital Technology by Children in Nigeria: Where are We?' *African Journal of Law and Human Rights (AJLHR*) (2025) 9(1) <http://SI SULEIMAN - African Journal Of Law And Human ..., 2025 - journals.ezenwaohaetorc.org> accessed 28 May 2025.

The expansion of the internet and its frequent use in day – to – day life with its easy access has made the children target and they are trapped by the abusers and become a victim of cyber pornography. Pedophiles explore this chance by providing their false identity on the net and make contact with the children in chat-rooms or via e-mails where these children are chatted for giving personal information about themselves. These pedophiles drag children to the internet for the purpose of sexual assault so as to use them as sex object. They lure children by pushing and providing them the pornographic material on the internet.[60]

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violate the privacy of that person.[61] It should be noted that these rights relates to every human being and most definitely children too and children being more vulnerable than adults need better protection against say cyber bullying which could take the form of discrimination, or violating privacy by service providers etc. thus in the digital space, a Childs right to privacy and have his correspondence and telegraphic communications are guaranteed and protected.[62]

Child pornography is a distinct criminal offence which when committed 'without right' and intentionally,[63] would lead to 10 years imprisonment or fine of not more than 20, 000, 000.00 or both where a person produce child pornography; offer or make available child pornography; and distribute or transmit child pornography.[64] While a term of not more than 5 years or a fine not more than 10,000,000.00 or both will be imposed on a person that procure child pornography for oneself or for another person; possess child pornography in a computer system or on a computer-data storage medium.[65]

The act of engaging in sexual activity with a child while using coercion, inducement, force, threats, abuse of a recognized position of trust, authority, or influence over the child, including within their family, or abuse of a particularly vulnerable circumstance of the child, constitutes grooming or soliciting a child through any computer system or network;[66] whoever violates the Act is subject,

[60] Vishwanath Paranjape, *Cybercrimes & Law*, (Central Law Agency, 2010) 4.
[61] Singh (n 47).
[62] Suleiman (n 59).
[63] Paranjape (n 60).
[64] Cybecrimes Amended Act 2024 (n 13) Section 23(1)(a) - (c).
[65] Ibid. section 23(1)(d) and (e).
[66] Promise Aaron, Miller Nzewenta and Damilola Abidoye, 'Digital Sexual Exploitation of Children in Nigeria: A Legal Discourse' *NAU.JCPL* (2024) 11(4) <http://journals.unizik.edu.ng> accessed 17 August 2025.

upon conviction, to a term of imprisonment of not more than 10 years and a fine of not more than 15, 000,000.00, or based on the offence committed, to a term of imprisonment of not more than 15 years and a fine of not more than 25, 000,000.00.[67] The Act went further to describe "child pornography," including pornographic content that graphically shows a minor engaging in sexual activity, a person who appears to be a minor engaging in sexual activity,[68] and realistic images of a minor engaging in sexual activity, while a "child" or "minor" is an individual who is under the age of 18.[69]

As discus above this Act criminalizes the production, distribution, and possession of child pornography, with significant penalties for those found guilty. However, the enforcement of these laws has been inconsistent, with challenges such as inadequate training for law enforcement officers and limited resources for investigation and prosecution hindering their effectiveness.[70]

1.3.10. Re-scoping the Parameters for the Offence of Cyber-stalking (Section 24).

Section 24 of the 2015 Act makes it an offence for any person to transmit a message via computer systems or networks that is grossly offensive, pornographic, indecent, obscene, or menacing, or knowingly send false information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent.[71]

This Section 24 of the 2015 Act has been a lightning rod for controversy since its inception. It has been criticized for its alleged role in curtailing and potentially undermining constitutionally guaranteed rights to freedom of the press and expression. This provision has been cited and used to justify alleged unlawful arrest of journalists and others based on their online activities.[72]

The reason for this is the fact that the section was termed vague and overbroad. Terms like "insult," "hatred," "inconvenience," "ill will," and "needless anxiety" were not clearly defined. What constitutes an insult, hatred, annoyance, or inconvenience under the section? Is there a limit to what may be classified under these terms? These ambiguities left the section open to interpretation,

[67] Cybercrimes Amendment Act 2024 (n 13) section 23(3).
[68] ibid. section 23(4)(a) - (c).
[69] ibid. section 23(5).
[70] Aaron, Nzewenta and Abidoye (n 66).
[71] Lawal, Ola and Chuma-Okoro (n 56).
[72] ibid.

allowing law enforcement agencies to target individuals arbitrarily. When a statute is vague, it gives undue power to prosecutors, leading to arbitrary enforcement.[73]

This provision has been used to quash freedom of expression since it was enacted. Its imprecise language makes it easy to target journalists, bloggers and media practitioners with inconvenient views. Many Nigerians have been harassed, intimidated, arbitrarily arrested and detained, and unfairly prosecuted for expressing views perceived to be critical of the government, whether at the federal or state level.[74]

In March 2024, reports emerged that the Economic Community of West African States (ECOWAS) Court of Justice ruled that Section 24 of the 2015 Act does not comply with Articles 9 of the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights. As a result, the ECOWAS Court of Justice ordered the Nigerian Government to amend section 24 of the 2015 Act.[75]

In reaction to the various criticisms, the Amended Act refined the language of Section 24 of the 2015 Act by limiting its parameters to pornographic or false information aimed at causing a breakdown of law and order or posing a threat to life. In effect, if a message is shown to be true and not pornographic, then no offence would have been committed under Section 24 of the 2015 Act as amended. This amendment is commendable; it represents a significant stride by the Nigerian Government in safeguarding the constitutionally guaranteed freedom of expression.[76]

Despite the changes introduced by the Amended Act and the ECOWAS Court of Justice's decision in March 2024, it has been reported that journalists are still being arrested, with law enforcement officers citing Section 24 of the 2015 Act as their authority. This is likely because the Amended Act fails to clearly define what constitutes a breakdown of law and order. This ambiguity allows law enforcement officers to use the law as a pretext to target journalists, claiming their actions amount to a breakdown of law and order.[77]

[73] ibid.
[74] Adeboye Adegoke, *Digital Rights and Privacy in Nigeria* (The Paradigm Initiative, 2020).
[75] Lawal, Ola and Chuma-Okoro (n 56).
[76] ibid.
[77] ibid.

The case of SERAP v FRN,[78] in ruling against Nigeria's indefinite suspension of Twitter, the Court held that blocking access to an online platform constitutes a violation of freedom of expression, particularly where such restriction is not proportionate, legal, or necessary in a democratic society. The Court also granted interim measures to restrain the government from harassing or intimidating citizens for continued use of Twitter, reinforcing the right to access digital platforms free from state coercion.[79]

This case marks a judicial turning point in African human rights jurisprudence, explicitly acknowledging digital rights as enforceable claims. It provides foundational legal grounding for future disputes involving Artificial Intelligence systems that may suppress or filter online expression. As Artificial Intelligence increasingly mediates digital communication, the principles affirmed in this case can be extended to ensure that AI-driven censorship or denial of access is subject to human rights scrutiny and judicial oversight.[80]

Cybercrime act putting journalist at risk (hunt journalist) In general terms, while Nigeria's Cybercrime Act came into effect to address genuine cyber-security issues, the enforcement of the law created serious human rights and freedom-of-press issues. Vagaries in the law's loose and sweeping provisions have been misused by the government in stifling critical voices, curbing digital expression, and silencing dissent. Widespread use of cybercrime law against journalists and activists emphasizes the urgent need for reforming the law balancing national security and the protection of basic human rights. Lacking clear protection measures and judicial intervention, the continued use of such a law threatens democratic values and Nigeria's commitment towards freedom-of-press and the protection of digital rights.[81]

A major problem raised by the Cybercrime Act is the implications of it for digital privacy and surveillance. The law provides the spy agencies an unbridled power to bug electronic communications, monitor trace data and private information with non-nix adjustment for judicial scrutiny. These provisions have further emboldened the surveillance on journalists, activists and

[78] *The Registered Trustees of the Socio-Economic Rights and Accountability Project (SERAP) & 3 ORS. v Federal Republic of Nigeria*, Application No: ECW/CCJ/APP/23; 24; 26 & 29/21 Judgment No: ECW/CCJ/JUD/40/22.
[79] Gladys Uzoamaka Eze and Peace Udoka Ogbonna, 'Judicial Perspectives on Human Rights and Artificial Intelligence: A Review of Decided Cases' *Nnamdi Azikiwe University Journal of Commercial and Property Law* (2025) 12(3) <http://GU Eze, PU Ogbonna - Journal of Commercial and Property ..., 2025 - journals.unizik.edu.ng> accessed 28 July 2025.
[80] ibid.
[81] Antai (n 21).

opposition politicians with more fear of curtailing digital rights along with freedom of speech. The possibility of authorities eavesdropping online communication was further magnified through intimidation and threats, which in turn confined the space for independent, unbiased media.[82]

Ambiguous assurances of government overreach have also primed fear that national security has been repackaged as the cloak for a top-down authorization of mass surveillance and totalitarian repression. The arrest and prosecution under Nigeria's cybercrime law have been done on reports from journalists, bloggers and activists on social media.[83]

One noteworthy provision is the court's authority under Section 24(3) of the Cybercrime Act to prevent further harassment. Section 24(3) of the Act provides that the court may, while sentencing, grant orders that may prevent further actions that may harass or cause reasonable apprehension in the victim.[84] The Legal ambiguity and vague legislative provision of section 24 for example, the criticism on cyberstalking and hate speech have still been criticized on misuse of freedom of expression.

1.3.11. Racist and Xenophobic Offences (Section 26).

Section 26 of the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 provides for racist, xenophobic, and genocidal offences online. Section 26(1) (a–b) criminalises the production and sharing of racist and xenophobic material with the public. Additionally, the offence includes threatening anyone based on their race, colour, descent, nationality, ethnicity, or religion.

Section 26 (1) (c), however, provides for the offence of insults based on these characteristics, while (d) criminalises genocide or crimes against humanity. Each of these offences carries various fines and imprisonment terms as punishments. But to what extent do these legal provisions include online hate speech? It is argued that, due to the fact that this cybercrime Act does not explicitly mention online digital platforms, the need to amend the Nigerian Cybercrime Act is necessary. The provision of Section 26 (1) (c) of the Cybercrime Act does not comply with international law in that "insults" are not covered under hate speech. For a speech to fall under the intention of

[82] ibid.
[83] ibid.
[84] Ifeoma E. Nwafor, 'Cyberstalking in Nigeria: An Exploratory Study of Section 24 of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024' *International Cybersecurity Law Review* (2024) 5 <http://IE Nwafor - International Cybersecurity Law Review, 2024 - Springer> accessed 19 July 2025.

Section 26 as labelled, it must fall under the strict prescription of international human rights law, as explained immediately above.

1.3.12. Liberalisation of the Scope of the Offence of Conspiracy, Aiding and Abetting (Section 27).

Under the 2015 Act, only employees of a financial institution were liable for conspiring, aiding and abetting the perpetration of fraud using computer systems.[85] However, the Amended Act broadens this scope to cover employees of both private and public organisations.[86] This move appears to have arisen from the recognition that cybercrime is not limited to the financial sector and that employees across various sectors can exploit computer systems and networks for fraudulent activities. The broader scope will indeed address the evolving landscape of cybercrime, ensuring comprehensive legal coverage and deterrence across all sectors.[87]

1.3.13. Manipulation of ATM/POS Terminals (Section 30).

The Principal Act restricted payment systems to Automated Teller Machines (ATMs) and Point of Sales (POS) terminals, overlooking various other payment technologies prevalent in Nigeria.[88] The limited coverage of the 2015 Act meant that fraudsters could exploit other payment technologies, such as mobile money payment applications, online banking platforms, contactless payment systems, and e-commerce gateways without facing legal consequences. This limitation necessitated an amendment to broaden the scope so as to ensure that all forms of payment technology are covered to provide comprehensive protection against fraudulent manipulation.[89]

The Amendment Act addresses this gap by holding individuals accountable for manipulating not only ATMs and POS terminals but also expanded the manipulation of ATM and POS terminals to include other payment technology means.[90] This expansion accommodates the diverse range of payment systems in Nigeria, ensuring comprehensive coverage and mitigating fraud risks associated with unconventional payment methods.

[85] Cybercrimes Act 2015 (n 48) Section 27.
[86] Cybercrimes Amended Act, Amendment section 6.
[87] Lawal, Ola and Chuma-Okoro (n 56).
[88] Cybercrimes Act 2015 (n 48) Section 30.
[89] Lawal, Ola and Chuma-Okoro (n 56).
[90] Cybercrimes Amended Act 2024 (n 13), Amendment Section 7.

1.3.14. Spreading of Computer Virus (Section 32(3)).

Section 32(3) is to the effect that, a person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of N1,000,000,.00 or both.[91]

The penalties must be reviewed to be stiffer than the current position. In April 2022, emerging computer virus were identified which further exacerbates cybercrimes. These include Mind ware, Black Basta and Onyx. These emerging malwares or ransom ware specifically target firms rather than individuals. The simple explanation for this is that firms and organizations are likely to be paid a higher sum by the cybercriminals as ransom because their data is confidential and crucial for continuous daily operations.[92]

1.3.15. Inclusion of the Requirement of National Identification Number (NIN) and Additional Means for Verifying Customers of Financial Institutions: (Section 37).

Previously, verification was limited to documents with the customer's name, address, and other relevant information before issuance of ATM cards, credit cards, debit cards and other related electronic devices.[93] The Amendment Act mandates that customers conducting electronic financial transactions at financial institutions must present their National Identification Number (NIN) issued by the National Identity Management Commission (NIMC) for identity verification.[94] In other word, the Amended Act mandates that financial institutions must verify the identity of their customers conducting electronic financial transactions and such customers must present their National Identification Number ("NIN") issued by the National Identity Management Commission, along with other valid documents bearing their names, before being issued ATM cards, credit cards, debit cards, or similar electronic devices. [95]

The NIN provides a high level of credibility and verification as it helps institutions to access verified and reliable information about their customers. The NIN aids in cutting down the time

[91] ibid. Section 32(3).
[92] Akindipe Dayo, 'Spate of Cybercrimes in Nigeria: Evidence of Gaps in the Legal Frameworks' *Adeleke University Law Journal* (2024) IV (1) <httP://aulj.adelekeuniversity.edu.ng> accessed 2 August 2025.
[93] Cybercrimes Act 2015 (n 48) Section 37 (1)(a).
[94] Cybercrimes Amended Act 2024 (n 13) Section 37 (1)(a),
[95] ibid. Amendment Section 8.

needed for verifying customers and helps financial institutions to better prevent identity fraud and ensure that only authorized individuals get access to financial services.[96] This requirement aims to expedite the tracking of defaulters or perpetrators using NIN, which contains individual data including physical addresses. However, there are concerns that implementation may face challenges, as defaulters could potentially create deceptive locations using authentic NINs.

1.3.16. Protection of Specific Traffic Data and Subscriber Information (Section 38).

The pervasive use of information and communication technology has made the use of personal data and their protection a big issue globally.[97] The 2015 Act merely required data retention and protection as prescribed by the relevant authority.[98] While the Amendment Act revises Section 38(1) of the Principal Act, aligning it with the Nigeria Data Protection Act (NDPA). Now, service providers are not only required to retain specified traffic data and subscriber information but are also mandated to ensure their protection in accordance with the provision of the NDPA and as may be prescribed by the Nigerian Communications Commission (NCC), for a period of 2 (two) years.[99] This amendment reflects the government's commitment to safeguarding data and subscriber information, reinforcing the agenda of data security and privacy.

Furthermore, 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 respected.[100]

However as mention above, scholars have also pointed to significant tensions between privacy rights and state surveillance powers embedded in these reforms. Laws mandating compulsory data

[96] Lawal, Ola and Chuma-Okoro (n 56).
[97] ibid.
[98] ibid.
[99] Cybercrimes Amended Act 2024 (n 13), Amendment Section 9.
[100] Cybercrimes Act 2015 (n 48) Section 38 (2) – (5).

retention or authorizing state interception of digital communications, have raised constitutional concerns regarding proportionality and necessity.[101]

1.3.17. Report of Cyber Threats, Co-ordination and Enforcement Through Sectoral CERTs or SOC Sectoral Security Operations Centres (Section 41).

Section 21 (1) and Section 41 (1) of the Principal Act are amended by Cybercrimes (Prohibition Prevention, etc) (Amendment) Act, 2024. Section 41(1)(d) – (h) are substituted while (i) and (j) are inserted by Cybercrimes (Prohibition Prevention, etc) (Amendment) Act, 2024.[102] The Act strengthens Nigeria's cyber security poster.[103] The Amendment Act establishes Sectoral CERTs and SOCs, which will collaborate with the National Computer Emergency Response Teams (CERT) as outlined in the Principal Act.[104] These Sectoral CERTs and SOCs are tasked with receiving information from individuals or institutions operating computer systems or networks, both public and private, in the event of cyber-attacks or disruptions.[105] Their primary responsibility is to promptly respond to such incidents.

Additionally, they will oversee the integration and routing of internet and data traffic from all public and private organizations to ensure the protection of the national cyberspace.[106] While section 21 (1) (reporting of cyber threats) is to the effect that, any individual or institution facing cyber-attack, intrusion, or disruption must notify the National CERT via their respective Sectoral CERTs or SOCs[107] within 72 hours of detection.[108] Failure to comply will result in denial of internet access and a mandatory fine of ₦2,000,000 (Two Million Naira) payable to the National Cyber-security Fund.[109] This swift escalation to the National CERT aims to mitigate cyber threats promptly, thus preventing disruptions of the cyberspace.

---

[101] Nazrul Islam Khan and Ishtiaque Ahmed, 'A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime nd Digital Evidence' *International Journal of Scientific Interdisciplinary Research* (2024) 5(2) <http://MNI Khan, Ahmaed - International Journal of Scientific Interdisciplinary ..., 2025 - ijsir.org> accessed 29 July 2025.
[102] Cybercrimes Amended Act 2024 (n 13), Amendment Section 10.
[103] O. M. Atoyebi, 'An Appraisal of the Cybercrimes (Prohibition, Prevention, Etc) Act (as Amended) 2024 and its Implications for the Nigerian Society' <httP://omaplex.com.ng> accessed 2 August 2025.
[104] Cybercrimes Amended Act 2024 (n 13), Amendment Section 10.
[105] ibid. section 21, and amendment section 3(a).
[106] ibid.
[107] Cybercrimes Amended Act 2024 (n 13) Section 21 (1).
[108] ibid. Section 21(3).
[109] ibid.

The Nigeria Data Protection Act (NDPA), 2023 established the Nigerian Data Protection commission.[110] It is the provision of the Act that where a personal data breach is likely to result in a high risks to the rights and freedoms of a data subject the data controller shall immediately communicate the personal data breach to the data subject in a plain and clear language,[111] and the report of data breaches is to be made to the Nigeria Data Protection Commission (NDPC) within 72 hours.[112] Thus, the commission is mandated to receive complaint relating to violation of the Act or subsidiary legislation under the Act.[113]

Additionally, Section 21 of the Cybercrimes Act requires businesses to report cyber-security incidents to the Nigeria Computer Emergency Response Team (CERT) or Security Operational Centres immediately to enable intervention as stated above. Failure to report within 72 hours attracts denial of internet service and in addition to pay N2, 000, 000.00 fine.[114]

The above have created legal ambiguity and potential conflicts in enforcement. Cybercrimes Act focuses at criminalising cyber offences while NDPA focuses at regulating the processing of personal data under section 40(3) of the NDPA the data controller required to immediately notify the data subject of a personal data breach which will likely result in high risks the freedoms and rights of the data subject.[115] This conflict could lead to confusion regarding which regulations take precedence where certain situation occur involving data or both cybercrime and data and how to deal with both simultaneously?

1.3.18. **Introduction of 2% of Annual Turnover Penalty for Failure to Pay Cyber (Section 44).**

Cyber-security Levy: Refers to a tax or fee imposed on organizations to fund cyber-security initiatives, such as; national cyber-security programs, cybercrime prevention and investigation, cyber-security research and development, information sharing and threat intelligence, Incident

[110] NDPA 2023 (n 11) Section 4.
[111] ibid. Section 40(3).
[112] ibid. Section 40(2).
[113] ibid. Section 5(g).
[114] Cybercrimes Amended Act 2024 (n 13) Section 21(3).
[115] Jumoke Lambo and others, *Data Protection Laws and Regulations Nigeria 2025* (2025) <http://iclg.com> accessed 23 September 2025.

response and disaster recovery. Cyber-security Levies can be implemented in various ways, such as, direct tax on organizations, fee on specific industries, surcharge on online transactions, etc.[116]

While taxation is essential for any country's survival, it is submitted that only a living citizen can fulfil tax obligation. However, Indeed, Nigeria's government faces a dilemma in balancing taxation with its primary responsibilities. The government's failure to protect citizens' lives and properties, provide jobs and implement laws that benefit Nigerians raise concerns. The country is struggling with inflation and citizens are finding it difficult to afford basic necessities.[117]

It is trite that since the enactment of Cybercrime (Prohibition and Prevention) Act in 2015, and imposition of the cyber-security levy under the Act, the cyber-security levy has never been enforced. The reason for non-implementation of the cyber-security levy stems from the fact that certain provisions in the Act, especially the amount payable as the levy, (0.005), the body to administer the levy, etc were vague and ambiguous. This led to the amendment of the Act in 2024 and the outcome of the amendment were; the specification of the amount payable as cyber-security levy.[118]

One of the Key changes made by the amendment Act which is relevant to this study include, the new amendment to section 44 (2)(a) to provide that; A levy of 0.5% (0.005) equivalent to a half percent of all electronic transactions value by the businesses specified in the Second Schedule to the Act shall be paid and credited into the National Cyber-security Fund (NCF). By this section thus, the amount payable as the cyber-security levy is clearly defined for ease of determination.[119] The specified businesses under the Second Schedule to the Act, are: (a) GSM Service providers and all telecommunication companies; (b) Internet Service Providers; (c) Banks and other Financial Institutions; (d) Insurance Companies; and (e) Nigeria Stock Exchange.[120]

In an attempt to ensure the implementation of the Cyber-security levy, the Central Bank of Nigeria, on the 6th of May 2024, published and issued a circular, providing "Implementation Guidance on

[116] Nwabachili Chioma O. and Nnoyelu Chinemelu V, 'Legality or Otherwise for The Imposition of Cyber Security Levy in Nigeria' *NAUJILJ* (2024) 16 (1) <http://www.ajol.info> accessed 19 July 2025.
[117] Peter Timi Omimakinde, 'Nigeria's Cybercrime Landscape: Examining the Trends, Patterns and Impacts of Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) 2024' (2025) 21(1) UNIZIK LAW JOURNA <http://journals.ezenwaohaetorc.org> accessed 2/8/2025.
[118] Nwabachili and Nnoyelu (n 116).
[119] ibid.
[120] Cybercrimes Amended Act 2024 (n 13) second schedule, Nwabachili and Nnoyelu (n 116).

the Collection and Remittance of the National Cyber-security Levy" (the "CBN Circular"),[121] to direct banks and other financial institutions to start charging a cyber-security levy on all banking transactions.[122] Cyber-security levy has brought several benefits for government, individual and businesses. However, there are also challenges and concern regarding the levy.

Unsurprisingly, this policy move raised concerns and drew sharp criticism for its perceived insensitivity and being inexplicably off-sync from the present realities of the average Nigerian trying so hard to make ends meet.[123] This guideline generated a lot of controversies, heated debates and unimagined resistance from stakeholders, legal practitioners, investors and even lawmakers. Many arguments raised issues like; the constitutionality or otherwise of the imposed cyber-security levy, the justification for the imposition of the levy in the light of Nigerian Economic Crisis as at the time the implementation is sought, the implication of the levy on investment in Nigeria, the actual person to bear the burden of the levy (whether businesses themselves or their customers), and the constitutional basis for the empowerment of the office of the National Security Adviser to administer the levy. The levy was criticized for being a way of milking a dying cow.[124] While some netizens have complained the high rate of levies being paid to Nigerian banks, some others accusing the present Nigeria's administration for lack of efficient economic strategies, while 'milking' the poor.[125] Others argue that, the measures of introducing the levy has blatantly contravene the Nigerian Constitution, the African Charter on Human and Poeples' Rights, and the International Covenant on Civil Political Rights.[126] Despite initial resistance and call for a suspension and review of the policy, the CBN has restated its resolve to enforce the levy.[127]

Under subsection (6) of the same section, the Office of the National Security Adviser is mandated to keep proper records of the accounts.[128] Additionally, Section 44(6) of the amended Act

[121] PSM/DIR/PUB/LAB/017/004 <http://www.cbn.gov.ng> accessed 6 August 2025.
[122] Chen Yizhen, 'Cybersecurity in Nigeria: Emerging issues, domestic governance and international cooperation' *World Journal of Advanced Research and Reviews* (2025) 26(2) <http://journalwjarr.com> accessed 5 August 2025.
[123] Mark Amaza, 'Cybersecurity Levy and Nigeria's Opaque Lawmaking Process' (13 May 2024) <http://dailytrust.com> accessed 27 July 2025.
[124] Nwabachili and Nnoyelu (n 116).
[125] Olayiwola Ajisafe 'This is extortion, Netizens lament CBN's new cybersecurity levy' Punch (Lagos, 7 May 2024) <https://punchng.com> accessed 18 August 2025.
[126] Ayodeji Adegboyega, 'Nigerians react to new 0.5% cybersecurity levy' Premium Times (Lagos, 7 May 2024) <https://www.premiumtimesng.com> accessed 18 August 2025.
[127] Temotope Aina. 'CBN eyes N50bn from Cybercrime levy' (20th September 2024) <http://punch.com> accessed 27 July 2025.
[128] Cybercrimes Act 2015 (n 48).

empowers the office of the national security adviser (ONSA) to establish a compliance monitoring system to monitor the deduction and remittance of the cyber-security levy[129] and the account of the Fund shall be audited in accordance with guidelines provided by the Auditor General of the Federation.[130]

The Act further provides other sources of funds for actualizing its objectives including; grants-in-aid and assistance from donor, bilateral and multilateral agencies; all other sums accruing to the Fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organizations,[131] and states clearly that all monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.[132] Furthermore, the Act provides that the levy imposed under subsection 2(a) shall be remitted directly by the affected businesses or organizations into the Fund domiciled in the Central Bank within a period of 30 days.[133] By subsection 44(5) an amount not exceeding 40 percent of the Fund may be allocated for programs relating to countering violent extremism. In addition, the new subsection (8) as amended is to the effect that, any business specified in the Second Schedule to the Act that fails to remit the levy under section 44 (2)(a) commits an offence and is liable on conviction to a fine of not less than 2% of the annual turnover of the defaulting business and failure to comply shall lead to closure or withdrawal of the business operational licence.

Currently there is serious on going argument as to the constitutionality or otherwise of the Cyber-security Levy in Relation to Section 162 of the Constitution. The principal issue for determination here is whether or not the Federal Government of Nigeria can maintain any other account other than the Federation Account for the purposes of receiving revenue collected by it?[134] Moreover, it is further argue that, the imposition of taxes without addressing significant threats like cybercrimes may be seen as misplaced priorities, cybercrime is a critical issue that the government should consider addressing, rather than using it as a means to generate revenue for the office of National Security Adviser. This is tantamount to a situation of robbing Peter to pay Paul. Hence, it is crucial

[129] Cybercrimes Amended Act 2024 (n 13).
[130] ibid. Section 44(7).
[131] ibid. section 44(2)(b) – (e).
[132] ibid. Section 44(3).
[133] ibid. Section 44(4).
[134] Nwabachili and Nnoyelu (n 116).

for the government to reassess its priorities and create a safer and more prosperous environment for Nigerians to survive.[135]

All the above issues led to the suspension of the implementation guided by Mrs. President, His Excellency, Bola Ahmed Tinubu for adequate consultation with and review by stakeholders. Since after the suspension, and up till the time of some researches, no further guideline has been issued on the enforcement of the cyber-security levy, hence the levy has been mere letters in the statute without any lifeline.[136] Thus, it is the view of this research still as of the time of writing this paper cyber-security levy remains contentious issue in relation to implementation and impact on the Nigerian citizens and Nigerian economy.

1.3.19. Elimination of Seizure of Passports and Order for Forfeiture of Assets (Section 48).

The Amended Act makes provision for deletion of Section 48 (4) of the 2015 Act[137] which requires (i) the cancellation of the international passport of a Nigerian convicted under the Act and (ii) the withholding of passports belonging to foreigners, which will be returned only after completion of their sentence or payment of fines.[138] This deletion is a welcome development. In another view, there is no reasonable justification and correlation between the commission of an offence under the 2015 Act, for which the offender will serve a jail term or pay fine, with the additional punishment of cancellation or withholding of passport.[139]

Section 48 is to the effect that, the court, in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeit to the Government of the Federal Republic of Nigeria.[140] Also section 48 makes provision in the interest of the victims where it provides for order for payment of compensation or restitution.[141]

[135] Peter Timi Omimakinde, 'Nigeria's Cybercrime Landscape: Examining the Trends, Patterns and Impacts of Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) 2024' *UNIZIK LAW JOURNA* (2025) 21(1) <http://journals.ezenwaohaetorc.org> accessed 2 August 2025.
[136] Nwabachili and Nnoyelu (n 116).
[137] Cybercrimes Amended Act 2024 (n 13) Amendment Section 12.
[138] Cybercrimes Act 2015 (n 48) Section 48(4).
[139] Lawal, Ola and Chuma-Okoro (n 56).
[140] Cybercrimes Amended Act 2024 (n 13) section 48(1).
[141] ibid. Section 49.

1.3.20. Jurisdictional Issue (Section 50).

The nagging question here is what happens when the Nigerian citizen's/resident's conduct constitutes an offence under the cybercrime Act of 2015 but it is not so under the foreign law? The requirement of section 50 (1) (c) of the Act presents an insurmountable challenge to the enforcement of the Act.[142] Lack of effective Cooperation between Nigerian Authorities and International Partners: Cybercrime is a cross-national and multi-jurisdictional phenomenon. Cybercrime is basically regarded as an international crime. This is because a successful prosecution of the crime often touches on various aspect of jurisdiction, hence, the introduction of Section 50 of the Principal Act to address issues on jurisdiction and international co-operation. One major setback in this regard is the fact that corruption and political interference have undermined efforts to investigate or prosecute cross-national crimes, such as cybercrime.[143]

1.3.21. Extradition (Section 51).

Section 51 is the effect that offences under the cybercrimes Act shall be extraditable under the Extradition Act, 2004.[144] However, the Cybercrime Act of Nigeria failed to consider the rules of extradition and the need for a mutual bilateral agreement between States before the extradition process can take place.[145] Since the enactment of cyber Act 2015, the Government has been committed to implementing reforms across various sectors, including the nation's cyberspace.

The 2015 Act which was enacted before the Policy addresses most of these concerns by providing penalties for breaches or disruptions to Critical National Information Infrastructure (NCII) and establishing timelines for cyber incident reporting. The act covers many offenses, including cyber fraud, identity theft, and cyberstalk, reflecting the Nigerian government's recognition of the economic and social impacts of cybercrime. Implementation and enforcement, however, remain significant challenges, exacerbated by limited resources and the need for international collaboration.[146] The Cyber Crime (Prohibition, Prevention, etc.) (Amendment) Act, 2024, in

[142] Abayomi B. Sogunle, 'Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement' *Journal of Law and Judicial System* (2021) 4(1) <http://sryahwapublications.com> accessed 2/8/2025.
[143] Omimakinde (n 135).
[144] Cybercrimes Amended Act 2024 (n 13).
[145] Kesiena Urhibo, 'Combating and Addressing the Menace of Cybercrime in Nigeria: An Overview of Applicable Laws' *AFJCLJ* (2021) 6 <http://www.researchgate.net> accessed 24 August 2025.
[146] Buçaj and Idrizaj, (n 1).

addition, reviewed the penalties for certain offences. However, the Amended Act does not allocate powers to the NCCC for coordinating national cyber-security and investigating cyber breaches.

1.3.22. Interpretation of Terms (Section 58).

The provision of section 58 of the Cybercrimes (Prohibition and Prevention) Act 2015 excluded smart or Internet of Things devices such as calculators from the definition of a computer.[147] The court also stated in National Advanced Systems v United States,[148] that a device is a computer if it is able to conduct calculations. In view of these courts' decisions, the Nigeria's jurisprudence should chart an innovative direction which should reflect in the legal landscape.[149]

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,[150] even though the word appeared twenty-five times throughout the pages of the Act. This implies that legislators do not understand cybercrime and the global community are already eliciting a universal definition of cybercrime.[151] It is the view of this paper that even with the amendment of the cybercrimes Act 2015 internet of thing is not included in section 58 of the Cybercrimes (Prohibition and Prevention) Act (as amended) 2024.

1.3.4. The Strength and Weaknesses of the Cybercrimes (Prohibition and Prevention) Act (As Amended) 2024.

Role of National Cybercrime Laws in Combating Cybercrime National cybercrime laws play a crucial role in addressing cyber threats by providing a legal framework for prosecuting cybercriminals, protecting data, and enforcing cyber-security standards. While national laws vary, they share common objectives: safeguarding public and private sectors from cyber threats, protecting individuals' personal information, and enabling law enforcement agencies to investigate and prosecute cybercrime effectively.

[147] Daniel Oluwadayo Akindipe and Olalekan Moyosore Lalude and Olaoluwatofunmi Tabitha Bamgbose, 'Appraisal of the Legal Framework on Emerging Cybercrimes and Virtual Disruption in Nigeria' *IEEE* (2024) <http://DO Akindipe, OM Lalude, OT Bamgbose... - 2024 IEEE 5th ..., 2024 - ieeexplore.ieee.org> accessed 29 July 2025.
[148] *National Advanced Systems v United States* (1994) Fed. Cir. 93-1496 (1994) 26 F.3d 1107.
[149] Akindipe, Lalude and Bamgbose (n 147).
[150] Uzoka and Umejiaku (n 36).
[151] D. Akindipe and D. Adeleke and C. David, 'The Universal Definition of Cybercrime: The Consequences of Incoherence,' *Adeleke University Law Journal* (2024) 4 (1).

Effective cybercrime legislation also encourages organisations to adopt cyber-security measures and promotes a culture of accountability and resilience. For instance, General Data Protection Regulation (GDPR) and similar data protection laws in other regions have incentivised companies to prioritise data protection, reducing vulnerabilities and improving overall cyber-security. National cybercrime laws form the foundation of a country's approach to cyber-security and cybercrime prevention. While these laws provide critical protections, they must adapt to the rapidly changing cyber threat landscape. As we proceed it is essential to recognise the strengths and limitations of national laws and explore how international cooperation can complement these frameworks to create a safer, more resilient digital ecosystem.[152]

Certainly, the Act criminalized cybercrime such as unlawful access to computers, unauthorized modification of computer systems, network data, computer associated forgery, computer related fraud and theft of electronic devices. The Act obviously provided for the modalities for holding internet fraudsters liable for internet fraud and crimes and never made any provision for the role of artificial intelligence in this regard.[153]

The Act succeeded in outlining the framework for investigating and prosecuting cybercrimes which relies heavily on digital forensics. However, the Act does not explicitly define forensic procedures. Though the Act mandate reporting cyber threat to National Computer Emergency Response Team (CERT) within 72 hours of detection. This prompt reporting is essential for appropriate investigations, which will include digital forensic analysis. Furthermore, even the National Cyber-security Fund established by the Act will likely be used to support digital forensic related activities, the presentation of NIN in electronic transaction as provided by the Act will serve as means of identifying perpetrators involved in cybercrimes.

Also, taking into consideration the scope of the offenses provided under part III all of which frequently requires digital forensic analysis and forensic evidence for investigation(which entails identification of perpetrator, method of access, nature of data obtain etc.) and prosecution. For example, if we take cyberstalking, sharing of child phonography, bullying, etc; digital forensic

[152] Onatuyeh (n 20).

[153] Osuji Emma, 'Interrogating the Challenges and Prospects of Artificial Intelligence in Cyber Crime Prevention nn Nigeria' *Rivers State University Journal of Public Law* (2024) 12(1) <http://www.rsupubliclawjournal.com.ng> accessed 2 August 2025.

palsy a critical role in tracing the origin of the communication and the identity of the individual involved.

It is the view of this paper that another crucial factor is that, the Act also does not explicitly address or regulate Artificial Intelligence in detail, provisions such as unauthorised access, data interception, and fraudulent activities may warrant the use of AI-driven cyber threat in certain situation. Therefore, there is need of improvement of digital forensics techniques to effectively supress cybercrimes.

1.3.5 Findings

1. AI-powered tools are among the means being used in committing cybercrimes offences. The paper found that no existing law in Nigeria that directly or expressly addresses, i.e, there is absence of AI-specific legal provision. The cybercrimes Act has not covered AI-related offense or addresses it misuse in the Act. Also, the Act does not contain forensic provisions on how to address cybercrimes when AI or computer related offences are involved.
2. It is the findings of the paper that, section 44 which imposed a 0.5%. Cyber-security levy on certain business transactions in Nigeria, stimulated a lot of controversy, to the extent that citizens argued that it goes contrary to the country's constitution provisions and also that government has imposed an additional burden that is severe.
3. The paper further finds that, the vagueness found in the Cybercrimes Act, in terms such as: 'valuable information', 'insult', 'hatred', 'inconvenience', 'ill will' and others as mentioned above, have has given room to ambiguities and disputes in comprehending their exact meaning. This has led to in arbitrary enforcement.
4. The paper found that there is lack of proper implementation of the Act due to enforcement challenges, i.e, the Act has come to be like a dog that barks but cannot bite. This can create problems for local businesses in Nigeria as well as foreign businesses who wish to employ digital sector.

1.3.6. Recommendations

1. The paper recommends that the Nigerian legislature should update and expand the provision of Cybercrimes Act 2024 and introduce clause that define AI system and criminalise their malicious use in cyber-relate offences. Thereby, covering all aspect when it comes cybercrime punishment, penalising individuals and organisations that deploy AI for illegal activities through the use of AI-driven technology. Furthermore, forensic provisions, establishment of forensic standards, building of specialised capacity to effectively investigate and prosecute AI-driven and computer offences should be updated. Also, the Nigeria's Government should involve in cross-border agreements to combat AI-driven cybercrimes effectively.
2. The recommendation of the paper is that, the government should the constitutionality, seek judicial or legislative clarification where necessary, hold consultation with civil society, businesses and financial institution to incorporate public input and review the 0.5% rate in order to adjust and minimize the hardship.
3. The paper recommend further that, the legislature should re-amend and clarify vague terms/ provisions in the cybercrimes Act 2024 and establish a review mechanism to prevent arbitrary application while preserving constitutional rights.

1.3.7. Conclusion

The impact of cybercrime is significantly detrimental, this phenomenon poses severe threats to the nation's technological, educational, political, security, and socio-economic advancement.[154] Despite the establishment of the aforementioned laws, the prevalence of cybercrimes in Nigeria remain distressingly high. The Nigerian Cybercrimes Act 2024 provides a significant landmark in the country's legislative effort to supress the development of cyber threat. The Act provides a comprehensive framework for addressing various forms of cybercrimes, including: Offences against critical national information infrastructure; Unlawful access to a computer; interception of electronic messages, e-mails, electronic money transfers; tampering with critical infrastructure; Computer related forgery; Computer related fraud; unauthorised electronic signature; Cyber terrorism, etc. in order to provide a safe digital environment for the Government, individuals and

[154] Ann Kuro John-Williams, 'Cybercrime and Economic Devlpment in Nigeria: Challenges, Opportunities, and Strategic Poicy Interventions', *African Journal of Social and Behavioural Science* (AJSBS) (2025) 5 (2) <http://AK John-Williams – African Journal of Social and …, 2025 – journals.aphriapub.com> accessed 7 September 2025.

businesses entities. However, there Act still faces criticisms and concerns remains about, enforcement challenges, jurisdictional issues, potential misuses, vague definition, need for review etc.