AN APPRAISAL ON THE LEGAL FRAMEWORK ON CYBERCRIME IN NIGERIA

By

O. H. Ordu*
A. N. Asuku**

Abstract

With greater connectivity and sophistication in the world, the goal of cyber attackers has been involving from traditional criminality to disruption economic activity and infrastructure. In some cases, the cybercriminals steal technical designs, defense and military secrets, university research findings and computer forensic investigation secrets instead of stealing information for pecuniary gains. With the arrival of information communication and technology, the world has now become a digital world, this has made communication and economic transactions easier, notwithstanding the advantages, development of the internet and the widened access of computer technology and has not only granted new opportunities for economic activities but has created opportunities for those involved in illegal activities. Cybercrimes are borderless crimes as they can be committed from anywhere at anywhere once the cybercriminals has interconnection or has access to computer device. Cyber laws deal with the codified rules that govern the exchange of communication and information for the protection of intellectual property rights, freedom of speech and public access to information in cyberspace. It refers to crimes committed by individuals using computers and internet. This work will attempt to examine the legal framework of cybercrime in Nigeria, classification and types of cybercrime. The main purpose is to examine what laws are in place to fight cybercrime and how efficient are the laws in Nigeria designed towards fighting cybercrime.

Introduction

The internet is one of the truly revolutionary technology in the information age in contemporary times. It has changed the way we live and work, and we have come to rely on it in every sphere of our endeavours, especially in the business world. Thus, the need to have cyber law to regulate the activities in cyber transaction cannot be overemphasized. This is crucial in order to curb the menace of cybercrime which has eaten deep into the fabrics of the society. Cybercrime is a kind of crime that happens in the cyber space in relation to computer and the internet, globally; and it

* Oroma Helen Ordu Esq, LLB (London); Email: oromalaw@gmail,com.
** Alaseikigimo Nahum Asuku Esq, LLB (UST, now RSU); BL (Abuja); Senior Magistrate, Bayelsa State Judiciary, Nigeria; Email: nahum.asuku@yahoo.com.

has serious potential for severe impact on our lives, society, and economy, because our society has graduated into information society where communication takes place in the cyberspace every now and then. This work will therefore examine the term or meaning of cybercrime, as well as appraise the legal framework on cybercrime or cyber laws in Nigeria and how efficient they have been designed to combat cybercrime in Nigeria. Accordingly, this paper will conclude by identifying some factors that will exacerbate cyber criminality in Nigeria and make certain recommendation to cure the situation in our society.

Meaning of Cybercrime

The word cybercrime can be understood by giving meaning to the words (cyber and crime) differently. The word 'Cyber' is a combining form meaning 'computer', 'computer network', or 'virtual reality', used in the formation of compound word. 'Cyber' refers to the science of communication that deals with the study of automatic control systems as well as mechanical-electrical communication system. Therefore, cyber is a derivative of cybernetics used to describe interaction that relate to, or involve computers or networks.

The word 'crime' refers to the specific actions or inaction due to negligence that is injurious to public welfare or morals and one that is legally prohibited. According to section 2 of the Criminal Code Act[1], *crime* as an act or omissions which renders the person doing the act or making the omission liable to be punish under the Act. According to Glanville Williams[2], *Crime* is 'a legal wrong that can be followed by criminal proceedings which results in punishment.' Cybercrime is a global phenomenon which takes place in the cyberspace. It is a crime carried out with the aid of computer systems. According to Haide and Jaishankar (2011)[3], cybercrime is an offence with a criminal motive, committed against an individual or group of persons intentionally to harm the reputation of the victims as well as cause irreparable damage to hardware of sensitive infrastructure, including internet and mobile phones. Theohary and Finklea (2015)[4] define cybercrime as crime committed using a computer network or hardware device. Sackson,[5] states that cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the internet. And the common health organization states that cybercrime includes not only crimes against computer systems (such as hacking, denial of service, cyberattacks and the setup of bonnets but also

[1] Criminal Code Act Cap C38 LFN 2004 (CCA).
[2] G Williams, *The Text Book of Criminal Law* (2nd edn Stevenson & Sons 1983) 27.
[3] Halder D and Jaishankar K, *Cybercrime and victimization of women: laws; Rights and Regulations* (Hershey PA USA IG Global 2011).
[4] C A Theohary and k Finklea, 'Cybercrime: Conceptual Issues for Conceptual Issues for Congress and US Law Enforcement' Congressional Research Service Report 2015https://digital.library.unt.edu/ark:/67531/metadc503621/: Accessed April 2022.
[5] M Sadeson, 'Computer Ethics: Are Students Concerned <http://webpages.cs.luc.edu/~laufer/ethics96/papers/sackson.doc > Accessed April 25 2020.

traditional crimes committed on electronic network (fraud via phishing and spam: illegal internet-based trade in drugs, protected species and arms) and illegal content published electronically, (such as child sexual abuse material).

Therefore, *Cybercrime* is any crime that involves the use computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Net crime is a criminal exploitation of the internet, inherently a cybercrime or computer crime. According to Broad hurst 2006[6]' cybercrime encompasses criminal activities which can be categorized by its unique typology of computer-related crime, comprising conventional crimes in which computers are instrumental to the offence. This is the case of intellectual property theft attackers on computer network; and conventional. Criminal cases in which abound undeniable evidence in digital form.

The act or omission is carried out by some criminal-minded individuals ('Yahoo Boys'), who indulge in the advance fee fraud schemes in Nigeria. Nigeria has therefore carved a niche for herself as the source of what is now popularly called 419. Nigeria now ranked first in African as the target and origin of cybercrime activities. Secondly, Ghana is also gaining prominence in cyber criminality being perpetrated by unscrupulous individuals called 'Sakawi Boys'. According to Maitarimi, the first reported cybercrime was committed by employees of a company in the 1960s and involved the company in mainframe computer[7]. Recently, it does not only involve employees of companies or nation, but include organized criminal gangs, terrorists, rogues, government and individuals. There are different classes of cybercrimes.

Classification of Cybercrime

Classification of cybercrime is an important step to fight against cybercrimes, hence it is statutorily provided under Cybercrime Act 2015, which has classified cybercrimes into three categories, namely: act carried out by criminal minded individual against computer; act carried out by criminal minded individual against people; and act carried out by criminal minded individual against state.[8]

Cybercrime Against Computer

Cybercrime against computer include cybercrime against all forms of property, such as computer vandalism, transmission of harmful programmes such as virus or denial of the service.

[6] Boradhurst P, 'Developments in the Global Law Enforcement of Cyber-Crime, Policing: An International Journal of Police Strategist and Management [2006] (29)(3) *Emerald Group Publishing Limited* 40, 408-433.
[7] O Maitanmi and Others, Impact of Cyber Crimes on Nigerian Economy (2013) (2)(4) *International Journal of Engineering and Science,* 45.
[8] Cybercrime (Prohibition and Prevention) Act 2015, s 2.

Cybercrime Against People

Cybercrime against people include various crimes like harassment of any one with the use of a computer such as email publishing, distribution, posting and dissemination of absence materials among others.

Cybercrime Against State

Cybercrime against state or government is seen as distinct kind of crime used by individuals and cyberspace against government as well as to terrorize the citizens of country. Cyber terrorism is one of the most common kind of crimes in this category, a crime which manifest itself into terrorism, when an individual cracks into a government or military maintained website.

Some Specific Types of Cybercrime

Some specific types of cybercrime include: cyber stalking, cyber terrorism, cybersquatting, password sniffing, phishing and spamming, wiretapping/illegal interception of telecommunication, fraud (identity theft), drug trafficking, yahoo attack (419), malware, pornography, and so on.

Cyber stalking

According to Ellison and Akdeniz[9], cyber stalking refers to the use of the internet, email or other electronic devices to stalk another person. Such crimes include internationally sending of mails via computer system that is grossly offensive or pornographic. It can be used interchangeably with online abuse or online harassment. The perpetrator does not present a direct physical threat to a victim, but follows the victim online activity, gathers information and eventually makes threats towards the victim. It includes where a person sends a false mail to another with an intention to annoy, inconvenience, obstruct, insult, cause criminal intimidation to another.

Cyber terrorism

According to Lewis (2002)[10], cyber-terrorism is the malicious act of using computer network to disrupt the normal processes of critical national infrastructures (such as energy, transportation, government operations), including the coercion or intimidation of public and private citizen. However, Hassan and Ors[11], described cyber extortion as a sort of cyber terrorism whereby the website, email server, or computer system leveraging on ransom ware is put under attack by

[9] L Ellison and Ors, 'Cyber Stalking: The Regulation of Harassment on the Internet' [1998] *Criminal Law review, Special Edition, Crime, Criminal Justice and the Internet* 28-48.
[10] *Ibid.*
[11] A B Hassan and ors, 'Cybercrime in Nigeria: Causes, Effects and the Way Out' [2012] (2)(7) *ARPN Journal of Science and Technology* 625-631.

hackers for denial of services and demand for ransom. A research carried out by[12] **XXX** defined cyber terrorism as an act of terrorism committed through the use of cyber space or computer resource. For instance, where a person intends to instill fear by accessing and distorting any useful information in organization or government bodies using computer and internet is generally referred to as cyber terrorism.

Cyber Squatting.

This type of cybercrime involves intentional use of a name, business name, trade mark, domain name or other word or phrase registered, aimed or in use by any individual, body corporate or in Nigeria, on the internet or any other computer network without authority or right and for the purpose of interfering with their use by the owner.

Password sniffing

To Hassan, password sniffers are programmes which are designed to collect the first 128 or more bytes of network connections within a defined network being monitored.[13] They are able to monitor all traffic on areas of network. The sniffers collect information when users type in information such as username and passwords, usually required when using common internet services and cover up their existence in an automated way.

Phishing and spamming

Phishing are high technology identity theft that steal personal information and identity of unsuspecting users as well as commits acts of fraud against the legitimate individuals or organization that have been victimized. While, spamming refers to unsolicited bulk electronic mail (email) and short message services (SMS) sent indiscriminately to prospective victims of crime via electronic messaging systems. Spam is the most practical cyber-attack weapon in Nigeria because of its low operating cost and difficulty that would be associated with holding anyone accountable for mass mailings.

For phishing, the perpetrators send false emails. It is fraudulently designed to mimic legitimate business, requesting for personal information which if released can allow them access one's bank accounts, including details of debit and credit cards. For the crime of spamming, the perpetrators, known as spammers, rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contracts.

Phishing/spamming refers to cloning product and e-commerce web pages in order to dupe unsuspecting users. It is a crime that the hackers use spontaneous mails to trick people into

[12] *Ibid*.
[13] *Ibid*.

disclosing their financial and/or personal data. The penetrators if found guilty shall be liable upon conviction to three (3) years imprisonment.[14]

Wire tapping/illegal interception of telecommunication

This crime refers to telephone fraud and is one of the major cybercrime perpetrated in Nigeria. With the increase in the use of cellular phones as well as the ability to purchase goods and services with credit cards over phones, the problem has increased dramatically in recent years. Criminals use wire tapping methods to eavesdrop on communications and gain access to information which they should not be privy to.

Fraud (identity theft)

This type of cybercrime refers to the act of depriving a person dishonestly of something, which such an individual is lawfully entitled to possess. According to Lseoghene[15] for fraud to be ascertained, there must be established a case of dishonesty, an intention to benefit on the part of the perpetrator at the detriment of other individual or organization. It is an act of deception deliberately carried out to gain unlawful advantage. For instance, making a false bank webpage to retrieve information of account of someone or calling and pretending to be who you are not with the aim of cheating the caller. This could range from black-hot hackers stealing online banking account login and password to get access to automatic teller machine (ATM). This type of cybercrime is very common in Nigeria.

Drug-trafficking

Drug trafficking is another prominent cybercrime which deals with global manufacturing, distributing and sale of prescription substances or drugs which are prohibition by law. Drug traffickers are increasingly taking advantages of the internet to sell their illegal substances through encrypted email and other internet technology.[16]

Yahoo Attack

This crime, otherwise known as 419 under the Criminal Code Act in Nigeria, is the number one types of cybercrime in Nigeria. To perpetrate this crime, the perpetrators uses email address obtained from the internet access points, harvesting applications (web spiders or email extractors).

---

[14] A S Gillis, *Phishing*<https://www.google.com/amp/s/www.techtarget.com/searchsecurity/definition/phishing%3famp=1> Accessed 28 Febuary 2022.

[15] J I Eseoghene, 'Bank Fraud in Nigeria: Underlying Causes, Effects and Possible Remedies' [2010] (6)(16) *African Journal of Accounting, Economics, Finance and Banking Research* 62-79.

[16] J Waggoner, Drug Trafficking and Drug Distributionhttps://www.finflaw.com/criminal/criminal-charges/drug-trafficking-distribution.html Accessed 30 Aprl 2022.

These tools can automatically retrieve email addresses from web page which may be used against unsuspecting victims.[17]

Malware

Malware are malicious software or code designed to by pass some security checks in computer or mobile devices and harness data without consent.[18] To Aviziens, Jean-Claude and Brian, it includes operational faults introduced into a system as viruses or worms.[19]

Pornography

This cyber offence covers all types of pornographic films and videotapes with varying degrees of sexual contents. The internet has provided a free market for this crime as so many pornographic sites are new all over the net. This is one of the most popular cybercrimes in Nigeria, particularly in academic institutions.

Legal Framework of Cybercrime in Nigeria

Some legal framework which regulates cyber criminality in Nigeria include the: Constitution of the Federal Republic of Nigeria 1999 (as amended); Nigerian Communication Act 2003; Criminal Code Act 2004; Penal Code Act 2004; Economics and Financial Crime Commission Act 2004; Advance Fee Fraud and other Fraud Related Offence (AFF) Act 2006; Money Laundering Act 2011 (now Money Laundering (Prevention and Prohibition) Act 2022); Evidence Act 2011; and the Cybercrimes (Prevention, Prohibition) Act 2015. Others include the Economic Community of West African State (ECOWAS) Directive on Fighting Cybercrime within ECOWAS; Economic Community of West African Union Convention on Cyber Security and Personal Data Protection; and so on.

Constitution of the Federal Republic of Nigeria 1999 (as amended) (CFRN)

The CFRN is the first point of call for cyber protection under the Nigeria legal jurisprudence. Section 37 of the CFRN provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected. Under the Constitution, the rights of individual are sacrosanct, and they can only be fettered or curtailed by extant laws made by a democratic government in the interest national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime for the protection of

[17] Criminal Code Act Cap C38 LFN 2004 (CCA), s 419.

[18] B Lutkevich, What is Malware https://www.google.com/amp/s/www.techtarget.com/searchsecurity/definition/malware%3famp=11 Accesed April 28 2022.

[19] Avizienis and Others, 'Dependability and Its Threat: A taxonomy' [2004] *Article IFIP Advances in Information and Communication Technology* 156.

the rights and freedoms of others. The constitution made provision on crime which enable the National Assembly to enact the Cybercrime Act 2015, accordingly.

Nigerian Communication Act 2003

This Act was enacted in 2003 with the primary aim of creating and providing a regulatory framework for the Nigeria telecommunication or communication industry.[20] Consequently, the Act does not provide for matters concerning cybercrimes. But it rather makes an obligation on the part of telecommunication providers to ensure that their network or facilities are not used to perpetrate crime.[21]

Criminal Code Act 2004

This Act, which is applicable in Southern Nigeria, criminalizes any type of stealing of funds in whatever form, and makes same punishable under the Act. Although cybercrime is not mentioned in the Act, yet it is a type of stealing punishable under the Criminal Code Act, which defines what constitutes an offence under the Act, and it provides that any representation made by words, writing or conduct of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe it to be true; is a false pretence.[22]

The most renowned provisions relating to cybercrime is chapter 38, which deals with obtaining property by false pretence. However the specific provisions relating to cybercrime is section 419, which states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen is guilty of felony, and is liable to imprisonment for three (3) years.[23] However, these provisions are actually not adequate to fight cybercrimes. This is because it does not contain any specific law prohibiting cybercrime, directly.

Penal Code Act 2004

This Act is applicable in Northern Nigeria. Like the Criminal Code Act, the law enforcement agencies rely on same to prosecute all criminal offences committed in Northern Nigeria, including stealing of any form. Sections 362 to 380 provide for the offense of forgery, section 179 make provision for impersonation. Whereas cheating and telecommunication offences are provided under sections 320, 325 and 334. It is to be noted that all offences including acts or omission classified as cybercrimes under the Budapest Convention are prosecuted by law enforcement

[20] Nigeria Communication Act 2003, s 1.
[21] *Ibid* s 146(1).
[22] Criminal Code Act Cap C38, s 418.
[23] Nigeria Communication Act 2003, s 146(1).

agencies under this Act[24] also. And there are some factors that exacerbate cybercrime in Nigeria, which include: lack of jurisdiction; lack of job; corruption, and so on. For example, in relation to jurisdiction, cybercriminals can sit in the comfort of their rooms and commit any form of cybercrimes which may adversely affect their victims in other jurisdictions. For instance, if Miss Helen in Nigeria commits an offence that had effect in the United Kingdom, there would be a problem on jurisdiction as to which country would try her for the offence.

Further, the poverty rate in Nigeria is another problem that had increases the rate of cybercrimes in Nigeria. The rate of poverty in Nigeria now is very alarming and has thrown our youth into indulging in all forms of cyber criminality, including graduates of higher institution due to lack of jobs to survive, hence, they indulge in cyber criminality to make ends meet.

Another factor which encourages and increases cyber criminality in Nigeria is corruption, which is also the bane in many African countries. However, the law provides that a person who engages in phishing would be liable upon conviction to 3 years' imprisonment. However, in Nigeria, when cybercriminals are caught, the police and prosecutor may demand for bribe, thus cases involving cybercrimes and cybercriminals may be closed or withdrawn by the police or prosecutor, as the case may be, without trial or with travesty of justice. Hence, corruption has enhanced the growth of interment crimes in the society.

Economics and Financial Crime Commission Act 2004 (EFCC Act)

This Act is enacted by the National Assembly for the protection and prevention of economic and financial crimes in Nigeria. And to promote the enforcement of its provisions, it also established the Economic and Financial Crime Commission (EFCC). In other words, it is the responsibility of the EFCC to investigate all financial crimes, including advanced fee fraud, money laundering, counterfeiting, illegal share, transfer, future market frauds, fraudulent encashment of negotiable instruments, computer credit card, fraud, contract scam, and so on.

It is, therefore, safe to say that the EFCC Act 2004, empowers the EFCC to investigate and prosecute perpetrators of cybercrimes in Nigeria, while placing reliance on the Advance Fee Fraud and Other Related Offences Act 2006. For example, in *Harrison Odiawa v Federal Republic of Nigeria*[25], the accused person who impersonated to be one Abu Belgore was arraigned by the EFCC on 58 counts of Conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering and possession of documents containing false pretence contrary to the Advance Fee Fraud and Other Related Offence Act. It was held by Hon. Justice J. O. K. Oyewole that from the evidence adduced by the prosecution, it is evident that the accused and his cohorts had a common intention to defraud Mr. George and acting in concert they did obtained the various sums of money

[24] Penal Code Act Cap P3 LFN 2004 (PCA).
[25] *FRN V. Harrison Odiawa* (2003 – 2010) ECLR 19-193; (2008 All FWLR (Pt 439) 436; (2008) LPELR CA/L/124/2006)

contained in the count charged and found guilty of the offences of conspiracy, forgery, uttering and in possession of documents containing false pretence. Section 7 of the EFCC Act 2004, thus equipped the Commission with the responsibility of enforcing the provision of the:

a) the Money Laundering Act 2004; 2003 No. 7; 1995 No.13;
b) the Advance Fee Fraud and Other Related Offences Act 1995;
c) the Failed Banks (Recovery of Debts and Financial Mal-practices in Banks) Act, as amended;
d) the Banks and Other Financial Institutions Act 1991, as amended;
e) Miscellaneous Offences Act; and
f) Any other law or regulations relating to economic and financial crimes, including the Criminal Code or Penal Code.[26]

Advance Fee Fraud and Other Fraud Related Offence Act 2006 (AFF Act)

This Act replaced the AFF Act 1995,[27] and it punishes 'advance fee fraud', otherwise known as 419; and the concept of 'advance fee fraud' Implies all fraudulent activities perpetrated with the intent of obtaining money from another person by false pretense.

According to section 20 of the Act, false pretense refers to 'a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe it to be true'. The Act provides, amongst others, ways to combat cybercrime and other related online frauds. Offences provided under the Act include: obtaining property by false pretence;[28] use of premises for fraudulent activities;[29] fraudulent invitation;[30] laundering of funds obtained through unlawful activity;[31] attempts,[32] conspiracy, as well as aiding and abetting.[33] There are cases decided by the Supreme Court relating to online advance fee fraud, including *Mike Amadi v Federal Republic of Nigeria*[34]. In that case, the Appellant (Mike Amadi) was charged before the High Court of Lagos State, Holden at Ikeja, by EFCC for an attempt to obtain the sum of US $125, 000.00 (One Hundred and Twenty Five Thousand United State Dollars) from one Fabian Fajans by sending fake email. In 2005, the High Court found him guilty and sentenced him to 16 years imprisonment. Dissatisfied with this decision, he appealed to the Court of Appeal,

[26] Economic and Financial Crimes Commission Act 2004, s 7(2).
[27] Advance Fee Fraud and Other Fraud Related Offences (AFF) Decree No.13 of 1993.
[28] Advance Fee Fraud and Other Fraud Related Offence Act 2006, ss 1 and 2.
[29] *Ibid, s* 3.
[30] *Bid, s* 4.
[31] *Ibid, s* 7.
[32] *Ibid, s* 5 and 6.
[33] *Ibid, s* 8.
[34] (2008) 12 SC (Pt III) 55; (2008) NSCQR 1127.

which affirmed the judgment of the lower court; and on further appeal to the Supreme Court, his appeal was dismissed and the judgements of the lower courts were affirmed.

Further, the Act also made certain provisions imposing certain duties on electronic communications service providers, such as telecommunications service providers, internet service providers and owners of telephone and internet cafes, to intercept or halt the use of the internet and telecommunications facilities by cyber criminals in perpetration advance fee scams. The Act also obliges any person or entity providing an electronic communication service or remote computing service, either email or any other form, to obtain the full names; residential addresses, in the case of individuals; and corporate addresses in the case of corporate bodies, from customers or subscribers.[35]

The Act also foist it upon any person or entity who engages in the business of providing telecommunications or internet services or the owner or person in the management of any premises being used as a telephone or internet café or by whatever name called to register with the EFCC; to maintain a register of all fixed line customers which shall be liable for inspection by any authorized officer of the EFCC, and also submit returns to the EFCC on demand on the use of its facilities.[36] And the essence of the compulsory registration with the EFCC is to facilitate the documentation of record of business engaged in the provision of telecommunications. In *Nnachi Ephraim v Federal Republic of Nigeria,*[37] the Appellant was charged by the EFCC and convicted by the Federal High Court, Kaduna Division, pursuant to the charges of operating prime Gate cybercafé at No. 1 Abakaliki, carryout internet and telecommunications services contrary to the provision of section 13(1)(a), punishable under section 13(5)(c) of the Advance Fee Fraud and Other Related Offences Act 2006; and the Appellant was found guilty by the High Court, and the decision was affirmed by the Court of Appeal.

Money Laundering Act 2011

This Act also makes provisions for the prohibition of the laundering of proceeds of crime or illegal act. Although cybercrime is not expressly mentioned in the Act, yet proceeds from cybercrime perpetrated by cybercriminals appear to be covered by section 15 of the Money Laundering Act 2022, which provides that:

> Money laundering is prohibited in Nigeria.[38] And any person or body corporate, in or outside Nigeria, who directly, indirectly, conceals or disguises the origin of converts or transfer; removes from the jurisdiction or argues, uses, retains, or take possession or control of any fund or property, knowingly, or reasonably out to have known that such fund or

[35] Advance Fee Fraud and Other Fraud Related Offence Act 2006, s 12(1).
[36] *Ibid* s 13(1)(a) and (b).
[37] (2012) LPELR – 22363 (CA).
[38] Money Laundering Act 2011, s 15(1).

property is, or forms part of the proceeds of an unlawful act, commits an offence of money laundering under this Act.[39]

Section 3 of this Act stipulates that bankers should identify their customers.[40] However, in-spite of such laudable provisions in the Act, financial and non financial institutions still provide vast opportunities for individuals and corporate bodies to attempt to engage or engage in carrying out money laundering activities.

Evidence Act 2011

The Evidence Act 2011 is the primary law in Nigeria which governs matter of evidence in judicial proceedings in Nigeria. Most juristic authorities actually define evidence as the means by which facts are proved, excluding inferences and arguments; or anything presented in court in support of an assertion. However, evidence is any relevant fact or set of facts accepted by the court, which proves or disproves any fact in issue in any judicial proceedings. The National Assembly repealed the erstwhile Act, which was enacted in 1943, but came into force in 1945, and survived until July 2011; and enacted the Evidence Act 2011, having a lot of novel provisions, including section 84, which is presently the extant law in Nigeria regulating the admissibility of computer and electronically generated evidence in judicial proceedings in Nigeria. Crimes committed with computer or internet often requires the tendering of computer or electronically generated evidence. And in most cases, the same is tendered by third parties, which ordinarily amounts to hearsay. However, section 84 appears to be an exception to the rule of evidence hearsay; while section 258(1) defines document to include books, maps, plans, graphs and so on;[41] any device sound is recorded;[42] any device sound and images are recorded;[43] and any device by means of which information is recorded, stored or retrievable, including computer output.[44] Prior to the Act in 1969, the Supreme Court in *Esso West Africa Inc v Oyebgola*[45] held, although obiter, that, 'the law cannot be and is not ignorant of modern business methods and must not shut it eyes to the mysteries of the computer'.[46] Although, the EA 2011 has provide section 84 for the admissibility of such evidence in court, it is not really sufficient to prove cybercrimes, as most acts of cyber criminality are perpetrated through computer, which may not produce hard copies of the actions involved in the crime, to prove the criminal actions or conducts involved.

[39] *Ibid, s* 15(2)(a) (b)(c) and (d).
[40] *Ibid, s* 3.
[41] EA 2011, s 258(1)(a).
[42] EA 2011, s 258(1)(b).
[43] EA 2011, s 258(1)(c).
[44] EA 2011, s 258(1)(d).
[45] (1969) NMLR 194.
[46] *Yesufu v ACB Ltd* (1976) 4 SC 1 at 9-14; (1976) NSCC 202 at 145 (SC).

Cybercrimes (Prevention, Prohibition) Act 2015

To supplement the provisions of the above Acts on cybercrime, as well as on the admissibility of electronic evidence on cybercrimes, the National Assembly enacted the very first indigenous Act to regulate matter of cybercrime in Nigeria, which is the Cybercrime Act 2015. In other words, this Act is the very first legal framework regulating the activities of persons in the cyberspace and cybercrimes in Nigeria.[47] This Act encapsulates the true and express intendment of the Act, demonstrating the deterrence theory of punishment. The Act is punitive in nature and this is as a result of the prevailing and escalating menace of cybercrimes in Nigeria. It provides a legal, regulatory and institutional framework for the prohibition, prevention, direction, investigation and prosecution and punishment of cybercrimes and other related matters. This Act offers an avenue of cyber security and consequently, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information infrastructure.[48]

More explicitly, the Act has 8 Parts with 59 Sections and 2 Schedules. Part 1 deals with the Object and Application of the Act, with two sections.[49] Part II deals with the Protection of Critical National Information Infrastructure, with three sections;[50] while Part III provides for the Offences and Penalties, in 31 sections;[51] some of which include: unlawful access to computer;[52] computer related forgery;[53] theft of electronic devices;[54] computer related fraud;[55] cyber terrorism;[56]cyber-stalking;[57] cybersquatting;[58] manipulation of ATM; POS terminals;[59] and so on. Part IV and V deal with the Duties of Financial Institutions;[60] as well as Administration and Enforcement,[61] respectively. Part VI deals with Arrest, Search, Seizure and prosecution, with 5 sections;[62] Part

[47] F Eboibi, 'A Review of Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015 (Forthcoming 2017) Computer Law and Security Review' [2017 *The International Journal and Technology Law and Practice on a Detail Review of the Nigerian Cybercrimes (Prohibition, Prevention) Act 2015*.
[48] Cybercrime Act, s 1.
[49] *Ibid* ss 1 and 2.
[50] *Ibid* ss 3-5.
[51] *Ibid* ss 6-37.
[52] *Ibid s* 6.
[53] *Ibid s* 8.
[54] *Ibid* 15.
[55] *Ibid s* 14.
[56] *Ibid s* 18.
[57] *Ibid* 24.
[58] *Ibid s* 25.
[59] *Ibid s* 39.
[60] *Ibid* ss 37-40.
[61] *Ibid* ss 41-44.
[62] *Ibid* ss 45-49.

VII deals with Jurisdiction and International Cooperation, with 7 sections;[63] while Part VIII deals with Regulations,[64] Interpretation,[65] and citation;[66] which terminates with the 2 Schedules.

Economic Community of West African State (ECOWAS) Directive on Fighting Cybercrime within ECOWAS

This is another very useful legal framework that is applicable in Nigeria, being a member of the ECOWAS. Further, ECOWAS upon recognizing the fact that the use of information and communication technologies and the internet has generated an up surge of reprehensible conducts within the region concerning cyber criminality, and that such acts and conducts require the identification of a legal regime and a suitable punishment because of the level of damage they generate or perpetrate; as well as the urgent need to adopt a framework for criminal liability for the purpose of fighting cybercrime effectively, at her Sixty-Sixth Ordinary Session of the Council of Ministers issued a Directive on Fighting Cybercrime within ECOWAS, and also urges member State to adopt necessary legislative, regulatory and administrative measure to comply with same,[67] hence this Directive on Fighting Cybercrimes within ECOWAS.

The Directive is divided into 7 Chapters, with 35 Articles. Article 2 provides for the Objectives of the Directive under Chapter I, which encourages member states to adopt a substantive and procedural criminal law of member states, with a view to addressing the menace of electronic crimes (otherwise known as cybercrimes), effectively. Thus, Chapters II-III provide for such offences, which include fraudulent access to computer access;[68] fraudulent input of data in a computer system;[69] computer data forgery;[70] use of data;[71] production of child pornography or pornographic representation.[72] Chapter V provides for the rules of procedure to tender such representations in evidence,[73] and the method of proof of such electronic offences.[74] And in compliance with this Directive, the National Assembly enacted the Cybercrime (Prohibition, Prevention, Etc) Act 2015 (a criminal law), and the Administration of Criminal Justice Act 2015 (an adjective law to guide prosecutors to prove

[63] *Ibid* ss 50-56.
[64] *Ibid* s 57.
[65] *Ibid* s 58.
[66] *Ibid* s 59.
[67] ECOWAS Sixty-Sixth Ordinary Session of the Council of Ministers Directive C/DIR/1/08/11 on Fighting Cybercrime within ECOWAS: Preambles 10-13; Art 35.
[68] *Ibid* Art 3
[69] *Ibid* Art 5
[70] *Ibid* Art 14
[71] *Ibid* Art 13
[72] The Directive, Art 16.
[73] *Ibid* Art 32.
[74] *Ibid* Art 32.

offences, which include computer and electronic offences perpetrated under the Cybercrime Act).

Economic Community of West African Union Convention on Cyber Security and Personal Data Protection

Like the ECOWAS, Nigeria is also a member state of the African Union (AU), which on 27 June 2014, at her 23 session of the submit of the AU in Malabo, Equatorial Guinea adopted the AU convention on cyber security and personal Data Protection, wherein members state were urged to adopt legal measures to curb cybercrime.[75] However, the AU convention is yet to enter into force because the requisite 15 countries ratification clause has not been achieved till date.[76]

Conclusion

Cybercrime is a major concern in Nigeria with regard to e-commerce. The rising spate of cybercrime globally and its attendant negative consequences has continued to call for immediate action in Nigeria to reduce the menace. There is no doubt that, although there have been some level of achievement recorded by the fraud prevention agencies such as EFCC and other law enforcement agencies in their effort in reducing cyber criminality in Nigeria, especially with the enactment of some relevant national legal framework for fighting cybercrime in Nigeria, including the Cybercrime Act 2015 (which has made extensive and express provisions on computer related fraud and forgery); yet the extant national legal framework in Nigeria is still inadequate in fighting cybercrimes in the Nigerian cyber environment.

Recommendation

Indeed, based on the above appraisal on the legal framework on cybercrime in Nigeria, couple with the inadequacies in the existing legal framework in fighting cybercrime in Nigeria, it is hereby suggested that:

a) The Criminal Code Act and the Criminal Code Laws of the various States in Southern Nigeria as well as its counterpart in Northern Nigeria be amended to include offences relating to cybercrimes, with stiffer punishment to ensure compliance.
b) More jobs be created in the country by government as well as platforms where the teeming unemployed youth who, otherwise engage in cyber criminality, may be trained to acquire desired entrepreneurial skills to build a career for themselves.
c) The National Assembly should enact related laws in addition to the Cybercrime Act 2015 to strengthen the cyber security legal framework in Nigeria.

[75] All convention on Cyber Security and Personal Data Protection, Art 35.
[76] *Ibid* Art 36.

d) The National Assembly should create a special court to prosecute only cybercriminals who commit cybercrimes in Nigeria for quick dispensation of justice.

e) The government should properly fund the institutional framework on cybercrime in Nigeria properly in order to promote enforcement and synergy in cyber security efforts.