Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.119, 2022


# Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations

Izevbuwa, Osaretin George[1] and Rita Abhavan Ngwoke[2]
1. Ph.D.; LL.M.; FICA; LL.B.; BL; professor of law
2. Senior Lecturer, College of Law, Igbinedion University Okada, Edo State, Nigeria
* E-mail of the corresponding author: okpeahior.rita@iuokada.edu.ng

**Abstract**
The creation of the internet, computers and mobile phones is one of the most innovative and useful inventions of man. There are inestimable benefits of these technological advances; businesses can be conducted and concluded between parties at different jurisdictions over the internet, correspondence between people have been made easier unlike what was the case of the 18th and 17th centuries where letters were used which was slow. In the same vein, the advances in technology has caused incalculable harm, it has increased the rate of crimes, expanded the scope of criminal activities and has created a new category of crimes known as cybercrimes. Cybercrime has in recent time become a crucial threat to many countries which has necessitated governments around the world to enact sturdy legislations and also put in place coherent procedural measures to tackle cyber-criminals. The Nigerian government enacted the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 to investigate and prosecute cybercriminals in Nigeria. Various other legislations also contain provisions that directly impact on the phenomenon of cybercrime in Nigeria. This paper utilized the doctrinal methodology to analyze the key provisions of the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 and other ancillary legislations on cybercrime in Nigeria with the aim of assessing their efficacy and providing possible solutions and recommendations to combatting the menace of cyber-crime in Nigeria.
**Keywords:** cybercrime, economic & financial crimes, money laundering, criminal code, prohibition, Nigeria
**DOI:** 10.7176/JLPG/119-01
**Publication date:**March 31st 2022

## 1. Introduction

Technology has brought together nations and the world has now become a global village.[1] Today, most countries rely on the internet to conclude important transactions that impact on their economies. Indeed, the arrival of Information Communication Technology (ICT) into many aspects of everyday life has led to the development of the modern concept of the information society.[2] Currently, there are 4.95 billion internet users and over 5.31 billion mobile phone connections worldwide. [3] According to a report given by the International Telecommunications Union (ITU), as at 2011, there were more than forty five million internet users in Nigeria, which is 26.5% of the population.[4] The recent statistics released by the Internet World Stats reveals that Nigeria ranks seventh in terms of countries with the highest number of internet users in the world and that Nigeria's total internet users stand at 115.99 million as at the end 2021.[5] This figure is projected to grow to over One 143.26 million internet users in 2026.[6]

Today, we live in the information Age –an age highly dependent on information resources, ideas and their practical applications rather than steel or coal, for development. Through cyberspace, one is able to communicate with virtually everyone in the world and economic transactions have now become relatively easier. Goods and services are routinely purchased and delivered electronically leading to significant changes in industries like journalism, travel and banking.[7] Indeed, economic development and national security now depends largely on the idea of a secured cyberspace.

Notwithstanding the advantages procured by the information age and the new tools of trade, the cyberspace remains a vulnerable domain in terms of national security, personal privacy, socio-economic and political

1 F. Okeshola and A. Adeta, 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria Kaduna State, Nigeria' (2013) 3(9) *American Journal of Contemporary Research* 98.
2 International Telecommunication Union (ITU) 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) September Report, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html accessed 14 July 2021.
3 DataReportal, 'Digital 2022: Global Overview Report', available at: https://datareportal.com/reports/digital-2022-global-overview-report accessed 11 March 2022.
4 International Telecommunication Union (ITU), above (n 2).
5 Statista, 'Number of Internet Users in Nigeria from 2017 to 2026', available at: https://www.statista.com/statistics/183849/internet-users-nigeria/ accessed 14 March 2022.
6 *Ibid*.
7 M. Olusola, 'Cyber Crimes and Cyber Laws' (2013) 2(4) *The International Journal of Engineering and Science* 19.

 

stability, and criminality. The growing convenience of the cyberspace comes at a cost. The development of the internet and the widened access to computer technology has not only granted new opportunities for economic activities, but has also created opportunities for those involved in illegal activities to thrive.[1] The flourishing connection between organised crimes and the internet increases the insecurity of the digital world.[2] The arrival of the internet has been pointed as the remote cause for lots of ingenious crimes hitherto unknown to our criminal law.[3] This has necessitated many countries to enact laws aimed at curbing the effect of criminality on the cyberspace. In Nigeria, the Cybercrime (Prohibition, Prevention etc) Act 2015 purports to prohibit, prevent and punish cybercrimes in the country, which has become hotbed of illicit activities on the internet globally.[4] This paper evaluates the legal framework for curbing the menace of cybercrimes in Nigeria to ascertain their efficacy and applicability.

## 2. Conceptualisation of Cybercrime

Cybercrime, a concept which to date has defied a globally accepted definition, appears to be the latest scourge plaguing humanity.[5] The word "cybercrime" is on the lips of almost everyone involved in the use of the computer and Internet. The substantive societal changes stemming from the development of computers, cellular telephony, and the Internet require clear definitions of what constitutes the abuse and misuse of internet technology. The definitions for such activities have evolved in tandem with technology itself to create a somewhat complex terminology.[6] As early as the 1970s, individuals used the term "computer crime" to refer to the misuse of computers and data.[7] During this same decade, one of the first computer crime laws in the US was passed in Florida in 1978, making all unauthorized access to computer systems a third degree felony.[8] The Internet existed at this time, though it was not well known or used outside of government, corporate, and university environments. Individuals who had the capacity to engage in computer crimes were generally employees working within a regulated environment who already had access to computerized data.[9] The term computer crime was most commonly used to refer to virtually all criminal activity involving computers until the late 1990s.[10] The terminology began to change as technology use and access fundamentally transformed society. The development of the Windows 95 operating system made computers much more user friendly, as did the ease of access to Internet connectivity.

Similarly, the creation of the web browser in the early 1990s, such as Netscape Navigator and Microsoft's Internet Explorer, allowed the home user to go online and experience content in a visual fashion through integrated images, text, audio, and video files.[11] Dial-up Internet service providers reduced the price of their services, and personal computers were sold with integrated modems and connection ports for phone lines or Ethernet cables for high speed connections. The global expansion of and connectivity a orded by the Internet led to the digitalization of sensitive financial and government information and massive accessible databases online. Financial service providers, social networking sites, and business platforms moved to online environments to o er services directly to home computer users, o ering convenient modes of communication and shopping.

As technology use patterns changed, researchers such as David Wall began to use the term "cybercrime" to refer to crimes performed online.[12] Grabosky,[13] however, used the term computer crime to refer to computer misuse. These terms were used relatively synonymously by researchers and journalists working during this period.[14] Though they technically recognize di erences in the role of technology in the course of an o ense, specifically, cybercrime refers to crimes "in which the perpetrator uses special knowledge of cyberspace,"[15]

---

1 O. Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber security in Nigeria' (2014) 6(3) *Academic Journal* 116.
2 N. Kshetri, 'Pattern of Global Cyber War and Crime: A Conceptual Framework' (2005) 11(4) *Journal of International Management* 541.
3 D. Ashaolu, 'Combating Cybercrimes in Nigeria' in D. Ashaolu, (ed.) *Basic Concepts in Cyberlaw* (Velma Publishers, 2012).
4 C.F. Izuakor, 'Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context', *ISSA Journal,* 2021, 28-29.
5 E. F. G. Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6(1) *Journal of Internet and Information Systems* 1.
6 Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses* (Routledge 2016).
7 D.B. Parker, *Crime by Computer* (Charles Scribner's Sons 1976).
8 R.C. Hollinger & L. Lanza-Kaduce, 'The Process of Criminalization: The Case of Computer Crime laws' (1988) 26 *Criminology* 101–126.
9 D.B. Parker, *Crime by Computer* (Charles Scribner's Sons 1976).
10 Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses* (Routledge 2016).
11 *Ibid*.
12 D.S. Wall, 'Digital Realism and the Governance of Spam as Cybercrime' (2004) 10 *European Journal on Criminal Policy and Research* 309–335.
13 P.N. Grabosky, 'Virtual Criminality: Old wine in New Bottles?' (2001) 10 *Social and Legal Studies* 243–249.
14 S. Furnell, *Cybercrime: Vandalizing the Information Society* (London: Addison-Wesley 2002) 21; T. Jordan, & P. Taylor, 'A Sociology of Hackers' (1998) 46 *The Sociological Review* 757–780.
15 *Ibid*.

 

while computer crimes occur because "the perpetrator uses special knowledge about computer technology".[1] By the mid-2000s, criminological researchers appeared to have adopted the term cybercrime to refer to technology-enabled o ending.[2] This is sensible as virtually all forms of computing, from mobile phones to MP3 players, are now Internet enabled. If all these devices can access the Internet, the potential for misuse in cyberspace increases dramatically. As a result of this technological change, we use the term cybercrime throughout the course of this paper to refer to o enses that can occur in online environments.

According to the Nigerian Communication Commission, cybercrime may generally be regarded as criminal offence involving a computer as the object of the crime (hacking, phishing, spamming), or as a tool to commit a material component of a crime (child pornography, hate crimes, computer fraud).[3] In simple terms, cybercrime may be explained as crime committed using the Internet. It is used to describe a range of offences including traditional computer crimes, as well as network crimes.[4] The word cyber-crime is a hybrid word. It is made of "cyber" and "crime". According to Sackson,[5] cyber-crime 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. Cybercrimes encompasses criminal acts that involves computers and networks.[6]

The Commonwealth Organisation states that cyber-crime includes not only crimes against computer systems (such as hacking, denial of service attacks and the setup of botnets) but also traditional crimes committed on electronic networks (e.g. 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).[7] The word cybercrime is popularly used to describe criminal activities related to cyberspace or the cyber world. Furthermore, the word cybercrime could be defined as any crime that involves computer and networks, including crimes that do not heavily rely on computers and most times the computer is either a tool or a target or both.[8]

From all the definitions of cybercrime above, we can say that cybercrime is crime carried out by criminal minded individuals or computers, enabled by criminals who use computers and internet enabled devices like smart phones, ipads, etc. to commit crimes through the internet from any location at any location. This is premised on the fact that cybercrimes are carried out by individuals or by computers programmed by individuals for the purpose of carrying out crimes. This definition also reflects the fact that cybercrimes are borderless crimes.

## 3. The Cybercrimes (Prohibition, Prevention, etc) Act 2015

The Nigerian Cybercrimes (Prohibition, Prevention, etc) Act 2015 is the first Nigerian cybercrime legal and regulatory framework enacted to regulate the activities of persons in the cyberspace and cybercrimes in Nigeria. The explanatory memorandum and objective of the Act encapsulates the true and express intendment of the Act, demonstrating the deterrence theory of punishment. The Act is punitive in nature, it provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution and punishment of cybercrimes and other related matters.[9] The Act is apportioned into 59 Sections; 8 parts; and 2 Schedules.

Part One of the Act contains Sections 1 and 2 of the Act. Section 1 provides for the objectives of the Act, which are the same with the explanatory memorandum of the Act. Section 2 of the Act provides that "the provisions of this Act shall apply throughout the Federal Republic of Nigeria".[10] Thus, no State House of Assembly can validly make any Law regulating Cybercrime in a State. This provision reinstates the doctrine of covering the field provided for in Section 4(5) of the Constitution of the Federal Republic of Nigeria 1999 (as amended), which provides that where a law enacted by the House of Assembly of a State is inconsistent with any law validly made by the National Assembly, the law made by the National Assembly shall prevail.

Part two of the Act contains sections 3 and 4, which provide for the protection of critical National

---

1 Wall, above (n 19) 335.
2 Holt & Bossler, above (n 17).
3 Nigerian Communication Commission, 'Final Report on: Effects of Cybercrime on Foreign Direct Investment and National Development,' 15 https://www.ncc.gov.ng/documents/735-nmis-effectscybercrime-foreign-direct-investment/file accessed 11 August 2021.
4 K.S. Chukkol, *The Law of Crimes in Nigeria* (Revised Edition, Ahmadu Bello University Press Ltd, 2010).
5 M. Sackson, 'Computer Ethics: Are Students Concerned' First Annual Ethics Conference (1996) <http://www.maths.luc.edu/ethics96/papers/sackson.doc> accessed 11 August 2021.
6 O. O. Oke, 'An Appraisal of The Nigerian Cybercrime (Prohibition, Prevention etc) Act 2015' <http://ssrn.com/abstract=2655593> accessed 11 August 2021.
7 Commonwealth Internet Governance Forum 'Commonwealth Cybercrime Initiative' http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA7786970A639B05%7D_Computer%20Crime.pdf accessed 11 August 2021.
8 D. Olowu, 'Cybercrimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa' (2009) 1 *Journal of Information, Law and Technology*.
9 Cybercrimes (Prohibition, Prevention, etc) Act 2015, explanatory memorandum.
10 *Ibid*, Section 2.

 

Information Infrastructure. Section 58 of the Act defines 'critical infrastructure' as systems and assets which are so vital to the country that their destruction would have an impact on the national security, economy, and public health and safety of the country. It is not necessary that the danger should be against the personal security of the head of state; a substantial threat to the critical national infrastructure is enough.[1] The President of the Federal Republic of Nigeria under Section 3 is empowered to designate computer systems as 'critical national information infrastructure'.

Part three contains Sections 5-36 of the Act.[2] This part contains offences punishable under the Act and penalties in respect of the offences. Section 5 of the Act prescribes the punishment for a person who commits an offence contrary to the critical national information infrastructure. Such person would be liable to 10 years imprisonment, but if the act causes bodily harm to any person, 15 years imprisonment. However, if the act causes death to another then life imprisonment.[3] The operational stability and security of critical infrastructure is vital for the economic security of the country, and hence its protection has gained paramount importance all over the globe.[4] The purpose of critical infrastructure protection is to establish a real time ability for all sectors of the critical infrastructure community to share information on the current status of infrastructure elements. Ultimately, the goal is to protect the country's critical infrastructure by eliminating known vulnerabilities and cyber-threats, which might graduate to cyber-terrorism.[5]

Section 6 of the Act criminalizes unlawful access to a computer. Section 6(1) provides that any person who without authorization, intentionally accesses in whole or in part a computer system or network for fraudulent purposes and obtain data that are vital to national security commits an offence and would be liable to 5 years imprisonment or fine not less than N5,000,000 or both. If the person has an intent to obtain computer data, the punishment is 7 years.[6] Section 6(4) protects computer, which affects private and individual interest within or outside the Federation of Nigeria. This section makes the application of the Act extra territorial.

Section 7 of the Act provides for registration of cybercafé. It provides that from the commencement of this Act all operators of a cybercafé shall register as a business concern with the Computer Professional Registration Council in addition to a business name registration with the Corporate Affairs Commission. This raises the issue of compliance and enforcement of this provision, the section did not expressly provide for any enforcement authority in charge of ensuring compliance by the owners of Cyber Cafes in Nigeria. Furthermore, most owners of cybercafé may not be aware of this requirements or even have the financial resources to register such businesses under Part C of the Companies and Allied Matters Act, 2004 (now Companies and Allied Matters Act, 2020) as such this provision might be dead in our statute books. A matter of equal concern is the position of a cybercafé, which is registered as a company under Part A of the Companies and Allied Matters Act. Should such cybercafé re-register as a business name under Part C of the Companies and Allied Matters Act?

Cybercafés are also directed under section 7(1) to maintain a register of users through a sign-in register. The register shall be available to law enforcement personnel whenever needed. Section 7(2) provides that any person who perpetuates electronic fraud or online fraud using a cybercafé shall be guilty of an offence and shall be sentenced to three years imprisonment or a fine of one million naira or both. Subsection (3) provides that if such person connives with the owners of the cybercafé, the owners would be guilty of an offence and sentenced to three years imprisonment or fine of one million naira.[7] Section 7(4) of the Act provides that, the burden of proving connivance shall be on the prosecutor. This is in line with Section 135(2) of the Evidence Act, 2011 which provides that:

> The burden of proving that any person has been guilty of a crime or wrongful act is, subject to Section 139 of this Act, on the person who asserts it, whether the commission of such act is or is not directly in issue in the action.[8]

Section 8 criminalizes the use of any computer system by any person without lawful authority.[9] Section 9 criminalizes the act of destroying or aborting electronic mails or processes which money or valuable information is being conveyed. It limits the punishment to only when money or valuable information is being conveyed. What is the standard of determining what a 'valuable information' is for the purpose of this Section? The Act under the definition section did not define what is 'valuable information'. The standard of determining what

---

1 M. O. Yusuf, 'Information and Communication Technology and Education: Analysing the Nigerian National Policy for Information Technology' (2005) 6(3) *International Education Journal* 316-321.
2 Cybercrimes (Prohibition, Prevention, etc) Act, 2015.
3 *Ibid*, Section 5.
4 Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical?* (Chatham House, Royal Institute of International Affairs 2013).
5 Y. Zahri, R. Ahmad, and M. Yusoff, 'Grounding the Component of Cyber Terrorism Framework Using the Grounded Theory' (2014) *Science and Information Conference* 523-529.
6 *Ibid*, Section 6(1).
7 *Ibid*, Section 7(3).
8 Evidence Act 2011, Section 135(2).
9 Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 8.

 

valuable information is should be on the part of the sender of the information, thereby making the standard subjective. This also makes other electronic mails which money or valuable information is not conveyed to be outside the protection of this section.

Section 10 of the Act criminalizes any act of an employee of Local Government, private organization or financial institution with respect to working with any critical infrastructure or electronic mail if the act is inconsistent with his contract of service. This provision of the Act attempts to regulate employment relationships between an employer and employee, however this regulation is only limited to employees working with any critical information. The rationale behind criminalizing an act of performing a role outside the scope of an employee's contract of service is still unclear. The section should have being modified to say that the employee must have had an intention to tamper with the critical information. Section 11 of the Act criminalizes the act of any person in willful misdirection of electronic messages.

Section 12(1) criminalizes the Act of unlawful interception of non-public transmissions of data. Subsection (2) criminalizes the act of any person who by false pretenses induces any local, state or federal government worker to deliver any electronic message to him, which is not specifically meant for him. Subsection (3) criminalizes the act of any Government worker who hides or detains any electronic mail and deliver same to wrongful person.[1]

Section 13 criminalizes the act of computer related forgery, which includes knowingly accessing any computer or network with the intention that such inauthentic data would be considered. Section 14 of the Act provides for computer related fraud. Section 14(4)(a) of the act provides that any person employed by or under the authority of any bank or other financial institutions who with intent to defraud, directly or indirectly, diverts electronic mails commits an offence and shall be liable on conviction to imprisonment. Section 14(4)(b) further provides that any person who commits an offence subject to subsection (4)(a) which results in material and/or financial loss to the bank or financial institution or customer shall in addition to the term of imprisonment, refund the stolen money or forfeit any property to which it has been converted, to the bank, financial institution or the customer.

This provision of remedial compensation for the victims of the crime is a novel provision under Nigerian Criminal Law. Remedial compensation for victims attempts to compensate them for crimes committed against them, as they would be entitled to damages if they had sued in a civil action. Section 15 of the Act criminalizes theft of electronic devices. It criminalizes the offence of stealing or attempted stealing of a financial institution or public infrastructure's terminal or an Automated Teller Machine.

Section 16 of the Act criminalizes the act of unauthorized modification of computer systems, network data and system interference. Section 17 of the Act provides for electronic signature. It provides that electronic signature in respect of purchases of goods and any other transactions shall be binding. However, the Act did not state the form such electronic signatures should be. Section 17(1)(b) provides for a procedural issue involving the genuineness of an electronic signature. It provide that the burden of proof lies on the person who asserts that an electronic signature does not belong to the purported originator of the signature. Section 17(1)(c) criminalizes the act of any person who forges another's signature or a company's mandate.

Section 17(2) removes from the list certain categories of document that would not be valid by virtue of the absence or irregularity of an electronic signature. These include, creation and execution of wills, codicils and or other testamentary documents, death certificate, birth certificate, matters of family law such as marriage, divorce, adoption or related matters, issuance of court orders, notices and official court documents.[2] This section is inconsistent with Section 93(2) of the Evidence Act which provides that:

> Where a rule of evidence requires a signature or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.[3]

This provision of the Evidence Act permits the use of electronic signature for any form of document while Section 17(2) of the Cybercrime Act removes certain documents from the purview of electronic signature.[4] This creates an inconsistency and problems of enforcement of such document in court. It has been argued that for evidential purposes, the provision of section 92 of the Evidence Act 2011 should prevail[5] because the Evidence Act 2011 is the foremost law on admissibility of evidence in Nigeria.

Section 18 of the Act criminalizes cyber terrorism, it provides that any person that accesses or causes to be

---

1 Ibid, Section 12(3).
2 *Ibid*, Section 17(2).
3 Evidence Act 2011, Section 93(2).
4 Wills, Codicils and or other testamentary documents; Death certificate; matters of family law such as marriage, divorce, adoption and other related issues; any cancellation or termination of utility services; issuance of court orders, notices, official court documents such as affidavit, pleadings, motions and other related judicial documents and instruments; any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; any document ordering withdrawal of drugs.
5 Ekhorutomwen Gabriel Ekhator, 'A Study of Electronic Signature and Its Legal Validity in Nigeria' (2020) 1 (1) *Lawrit Student Journal of Law* 47.

 

accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.[1] The Act adopted the definition of Terrorism as provided under the Terrorism (Prevention) Act, 2011 (as amended 2013). Section 1 of the Terrorism Act defines terrorism as an act which is deliberately done with malice and may seriously harm or damage a country or an international organization.[2] The Amendment to the Act expanded the definition of terrorism to include the act of financing any terrorist group.

Section 19 of the Act imposes a duty on financial institutions to safeguard sensitive information of their customers and prohibits them from giving a single employee access to sensitive information.[3] Section 19(3) provides that financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information. Where a security breach occurs the proof of negligence lies on the customer to prove that the financial institution in question could have done more to safeguard its information integrity. This provision accords with the burden of proof in criminal cases, which is on the prosecution to show that the defendant is guilty, this burden on the customer might be difficult to discharge because of lack or inadequate information at the disposal of such customers. Section 20 criminalizes the act of any employee of a financial institution who with intent to defraud issues false electronic or verbal messages.

Section 21 imposes a duty on any one operating a computer system to notify the National Computer Emergency Response Team (CERT) of any attacks or intrusion on its computer. This is one of the enforcement bodies created by the Act to enforce its provisions. Any person who fails to report such incident shall be liable to pay a mandatory fine of ₦2, 000,000 million to the National Cyber Security Fund. This section imposes a duty on anyone to report any crime committed under the Act to the CERT and failure to report the crime in itself constitutes a criminal offence and such person will be liable to pay a fine. However, the Act did not state how and where the CERT will be contacted and the procedure for contacting the CERT.

Section 22 of the Act criminalizes identity theft and impersonation of any person who is engaged in the services of any financial institution. Section 23(1) of the Act criminalizes the act of using child pornography on any computer system or network. Section 23(3) criminalizes the act of using any computer system or network for the purpose of meeting a child and engaging in sexual activities with the child. This brings into the ambit of the Act, the use of social media such as Facebook, Twitter, Instagram and the numerous social media platforms to meet a child and engage in sexual activities with the child. The definition of computer system in the Act is wide enough to cover portable handset and other communication devices. The Act under Section 23(5) defines child or minor as a person below 18 years of age.

Section 24 of the Act deals with cyberstalking, it criminalizes the act of any person who sends offensive materials to another through a computer network. Section 24(3) of the Act empowers the court to make any order necessary for preventing any act of further harassment on the person concerned. Subsection (5) provides that the order may last for a specified period and the defendant may apply to the court to vary the order. The court is also empowered to make an interim order for the protection of victims from further exposure to the alleged offences. This is a laudable provision of the Act, as it provides not only for the punishment of the offender but to protect the victim of the offence from further acts of cyberstalking from the offender.

Section 25 of the Act provides for cybersquatting. This is a welcome development as this section protects intellectual property rights on the internet and cyberspace. The practice of cybersquatting generally refers to abusive domain name registration, offering for sale or using an internet domain name which incorporates someone else's trademark, name or existing business or other company designation in order to block the domain, sell or license it with the intent of profiting from it.

Section 25(1) provides that any person who intentionally takes or makes use of any name, business name, registered and owned by any individual or government without authority or right, commits an offence. In awarding penalty against the offender, the court is to have regard to any refusal of the offender to relinquish, upon formal request by the rightful owners and an attempt by the offender to obtain compensation in any form for the release to the rightful owners for use of the name. In addition to the penalty, the court may also order that the offender relinquish such registered name, mark, trademark, domain name or other word or phrase to the rightful owner. This extends the protection of intellectual property from physical to the cyberspace.

Section 26 of the Act criminalizes the act of using any computer system or network to promote racist and xenophobic attacks. The Act under Section 26(1)(c) criminalizes the act of public insult of persons for reasons that they belong to a group distinguished by race or colour through a computer system or network. This is taking the provisions of the act too far as it is common in Nigeria to find members of different ethnic group in a verbal exchange directly or through the internet. The provisions of this Section can be modified to read that if such insults are done for the purpose of inciting violence against members of other ethnic groups. This section also prohibits acts that justify genocide and crimes against humanity.

1 Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 18.
2 Terrorism (Prevention) Act 2011, Section 1.
3 Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 19.

 

Section 27 criminalizes the act of any person who attempts to commit an offence under the Act or aids and abets another in committing an offence; such person shall be liable for the same punishment as the principal offender. Section 27(2) criminalizes the act of any employee of a financial institution who is found to have connived with another person to perpetuate fraud, such person is liable to seven years imprisonment and to return the money converted to the Bank. Section 28 of the Act criminalizes importation and fabrication of e-tools, including computer program or component designed or adapted for the purpose of committing an offence under the Act. Section 29 criminalizes the act of breach of confidence by service providers, where the computer based service provider with intent to defraud, illegally uses its customers security code with the intent to gain any financial or material gain. The Act also provides that where a body corporate is convicted of an offence under the Act, the court may order that the body corporate be wound up and all its assets and properties forfeited to the Federal Government. This provision expands section 406 of the Companies and Allied Matters Act, which provides for compulsory winding up of a company. However, such body corporate may not be liable if it proves that it had no knowledge of the offence and that it exercised due diligence to prevent the commission of the offence. The burden of prove in criminal offences is always on the prosecution, however this section places the burden of proving the offender's innocence on him, a position that offends the principle of burden of proof under Nigerian Criminal Law.

Section 30 of the Act criminalizes the manipulation of an ATM machine or point of sale terminals. Section 31 mandates every employee to surrender to its employer codes or access rights immediately they leave the employment of the employer but this provision is without prejudice to any contractual agreement between the employer and the employee. Section 32 of the Act criminalizes the offence of Phishing and spamming and also spread of computer virus. Phishing is defined under the Act as the criminal and fraudulent process of attempting to acquire sensitive information such as usernames and password.

Section 33 of the Act deals with electronic cards and related fraud, the section attempts to criminalize any act of tampering with any of credit, debit, charge and other types of financial cards. The section criminalizes the act of stealing an electronic card. Section 34 criminalizes the act of dealing with another person's card. Section 35 criminalizes the act of selling by an unauthorized person of cards and purchase of such cards. Section 36 of the Act criminalizes the use of fraudulent device or attached emails to obtain information or details of a cardholder.

Part Four of the Act contains Sections 37 – 40 of the Act. Section 37 of the Act imposes a duty on financial institutions to verify the identity of their customers before issuance of any form of card or electronic devices. The Act defines a financial institution as any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities. Section 37(3) imposes a duty on financial institutions to reverse within 72 hours any unauthorized debit made on the account of a customer, failure of which constitutes an offence. This provision also stretches the regulatory powers of the Act to the operations of Banks and Financial Institutions whose operations are already governed by the Central Bank of Nigeria Act[1] and the Banks and Other Financial Institutions Act (BOFIA).[2] This creates an overlap in the application of the Acts. The Banks and Other Financial Institutions Act has placed the supervision of Banks and Financial Institutions under the purview of the Central of Bank Nigeria.

Section 33 of BOFIA gives the Governor of the Central Bank of Nigeria the power to order a special examination or investigation of the books and affairs of a Bank where he is satisfied that it is in the public interest to do so or that the bank has been carrying on business in a manner detrimental to the interest of its depositors and creditors.[3] Hence, the provisions of the cybercrime Act that regulate the relationship of financial institutions with their customer is inconsistent with the provisions of BOFIA. An interesting provision of the BOFIA is section 55 and 56 which provides that where the provisions of the Companies and Allied Matters Act or Nigeria Deposit Insurance Corporation Act is inconsistent with the provisions of the BOFIA, the provisions of the latter shall prevail.[4] The question is whether the same provisions of BOFIA can override the above provisions of the Cybercrime (Prohibition, Prevention etc) Act. This appears to be the position of the Supreme Court decision in *Federal Republic of Nigeria v Osahon*,[5] which states that where two Acts of the National Assembly are in conflict the Act that is particular on the subject shall prevail.

Sections 38, 39 and 40 of the Act discusses the duties of service providers, who are defined under the Act as any public or private entity that provides to users its services, which include the ability to communicate by means of a computer system, electronic communication devices, or mobile networks. It also includes any entity that processes or stores computer data on behalf of such service providers. It imposes a duty to retain all subscriber information for a period of 2 years and such information shall only be release to regulatory agencies

1 Central Bank of Nigeria Act, Cap C4, Laws of the Federation of Nigeria, 2004.
2 Banks and Other Financial Institutions Act 2020.
3 *Ibid*, Section 33.
4 *Ibid*, Section 55 and 56.
5 (2006) 5 NWLR (Pt. 973) 361.

 

who shall have regard to an individual's right to privacy under the constitution.[1]

Section 39 imposes a discretionary duty on a judge to grant access to information of a subscriber for a criminal investigation only. Section 40 of the Act imposes a duty on the service provider to work with law enforcement agencies and prescribes it as a criminal offence for failure to do so. The activities of service providers is also regulated by the Nigerian Communications Commission Act[2] and pursuant to the powers vested in the commission under Section 70 of the Act it published the Nigerian Communications Commission (Registration of Telephone subscribers) Regulation, 2011. This regulation prescribes the method of keeping data of telephone subscribers in Nigeria. Section 8 provides that notwithstanding the provisions of the Regulation restricting access to subscriber information on the central database and subject to the provisions of any Act of the National Assembly, subscriber information on the central database shall be provided only to security agencies; provided that a prior written request is received by the commission from an official of the requesting security agency who is not below the rank of an assistant commissioner of police or a coordinate rank in any other security agency.[3] This provision can be read alongside the provisions of the Cybercrime Act, to state that such subscriber information can only be released at the request of the relevant authority or law enforcement agency if there is a written request by an official of the requesting security agency who is not below the rank of an Assistant Commissioner of Police.

Part Five contains sections 41 to 44 of the Act. Section 41(1) designates the office of the National Security Adviser as the coordinating body for all security and enforcement agencies under the Act. It imposes several duties on the body, one of which is to provide all relevant security and intelligence for combating cybercrimes in Nigeria.[4] It also mandates the office to establish and maintain a National Computer Emergency Response Team (CERT) and the National Computer Forensic Laboratory. It imposes a duty on the Office of the National Security Adviser to coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global framework on cyber security.

Section 41(2) of the Act imposes a duty on the Attorney General of the Federation to enhance Nigeria's cybercrime and cyber security law with international standards and maintain international cooperation for preventing and combating cybercrime. Another laudable provision of the Act is that it requires all law enforcement agencies to organize training programmes for officers in charge of the prohibition, prevention, detection, investigation and prosecution of cybercrimes. This makes it more effective for the law enforcement agencies under the Act to detect, prohibit and prevent cybercrimes in Nigeria.[5] Section 42 of the Act also establishes the Cybercrime Advisory Council, which is enjoin to meet four times a year and shall be presided over by the National Security Adviser. Section 43 of the Act listed the duties of the Council, one of which is to create an enabling environment for members to share knowledge and promote the study of cybercrime detection.

Section 44 of Act establishes the National Cyber Security Fund and the monies that will be kept in the funds includes a levy of 0.005 of all electronic transactions by businesses specified in the Second Schedule to the Act, gifts and grants. The businesses stated in the Second Schedule includes GSM service providers and all Telecommunications Companies, Internet service providers, Banks and Other financial institutions, Insurance Companies and the Nigerian Stock Exchange.[6] Part six contains Sections 45 – 49 of the Act. Section 45 provides that a law enforcement officer is to apply *ex parte* to a Judge for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation. This section also establishes criminal procedure rules which are already enacted in the Administration of Criminal Justice Act. Under the Administration of Criminal Justice Act, a magistrate can issue a warrant to a law enforcement officer to search or obtain evidence in a premises.

Section 46 makes it a criminal offence to obstruct any law enforcement officer in the performance of his duty under the Act. Section 47 provides that relevant law enforcement agencies shall be in charge of enforcement of the Act subject to the powers of the Attorney General of the Federation. Section 48 imposes a discretionary duty on the Court to order a person convicted of an offence under the Act to forfeit to the government of Nigeria any proceeds from the offence. If the convicted person has assets in a foreign country subject to treaties between Nigeria and the foreign country, the assets shall vest in the Federal Government of Nigeria. Section 49 of Act also directs that the Court may order a convicted person to return to the victim of the offence the item lost by the victim.

Part seven contains sections 50 – 56 of the Act. Section 50 of the Act vests jurisdiction over offences committed under the Act on the Federal High Court regardless of where the offence is committed in Nigeria: in a ship or aircraft registered in Nigeria, by a citizen or resident in Nigeria – if it would constitute an offence under a

[1] Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Sections 38.
[2] Nigerian Communications Commission Act, Cap. N97, Laws of the Federation of Nigeria, 2004.
[3] Nigerian Communications Commission (Registration of Telephone subscribers) Regulation, 2011, Section 8.
[4] Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 41(1).
[5] *Ibid*, Section 41(2).
[6] *Ibid*, Section 44.

 

Law of the Country where the offence was committed, or outside Nigeria where the victim of the offence is a citizen or the alleged offender is in Nigeria and not extradited. This raises conflict of Law issues and it is against the established principle of International Law that a criminal is prosecuted where the offence is committed.

Section 51 provides that offences created under the Act shall be extraditable under the Extradition Act.[1] Section 1 of the Extradition Act provides that where a treaty or other agreement has been made by Nigeria with any other country for the surrender of any persons wanted for prosecution or punishment, the National Council of Ministers may by order published in the Federal Gazette apply this Act to that country.[2] This enhances international co-operation in fighting cybercrimes.

Section 52 of the Act empowers the Attorney General to partner with any foreign state to investigate or prosecute offences under the Act.[3] Section 53 of the Act provides that evidence obtained in a foreign country can be used in court proceedings in Nigeria if such evidence is authenticated by a judge, magistrate or Justice of Peace, or by the seal of a ministry or department of the Government of a foreign state. This section is also inconsistent with the provisions of the Evidence Act regarding admissibility of foreign evidence.[4] Section 106(h) of the Evidence Act[5] provides that foreign evidence can be used in Nigeria where it is a copy and it is sealed by a foreign or other court to which the original document belongs or be signed by a Judge. It can be certified by a notary public or a consul or diplomatic agent and shall be admitted upon proof of the character of the document according to the law of the foreign country. This Section of the Evidence Act expands the scope of persons who can certify foreign evidence from those provided under the Cybercrime Act. Section 54 of the Act prescribes the ways which a foreign country can request for evidence in Nigeria.

Section 55 provides for expedited preservation of computer data. Section 56 mandates the National security adviser for the purpose of international cooperation to make available a contact point twenty four hours a day. It provides that the contact point shall be reached by other countries of other contact points in accordance with agreements, treaties or conventions.

Part eight contains Sections 57 – 59 of the Act. Section 57 provides that the Attorney General may make rules or regulation for the purpose of the efficient implementation of the provisions of the Act.[6] Furthermore, any lacuna in the Act can be cured by a regulation made by the Attorney General of the Federation. Sections 58 and 59 provides for the definition of terms and citation of the Act respectively.

The First Schedule to the Act states the members of the Cybercrime Advisory Council, list of ministries and departments and agencies who are to bring representatives from each of them to represent the ministry in the advisory council. The Second Schedule to the Act provides for the businesses which Section 44(2)(a) of the Act refers to.

## 4. Other Ancillary Laws against Cybercrime in Nigeria

### 4.1 The Economic and Financial Crimes Commission Act (EFCC Act) 2004

The Economic and Financial Crimes Commission Act (EFCC Act) established the Economic and Financial Crimes Commission (EFCC) to combat all economic and financial related crimes in Nigeria. The EFCC Act was repealed and reenacted as the Economic and Financial Crime Commission (Establishment) Act 2004. The Act confers special powers on the Commission to investigate any person, corporate body, or organization who has committed any Act relating to economic and financial crimes.

Section 5 of the Act charges the Commission with the responsibility of the enforcement and the due administration of the Act, the investigation of all financial crimes including, advance fee fraud, money laundering, counterfeiting, and illegal charge transfers. It is also charged with the prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation. Criminal activities that come under these economic crimes include the activities of the "Yahoo boys" who commit cross-border cyber offences capable of sabotaging the economies of country.[7] Section 5 has been the basis of various arrests and prosecution by the EFCC, including in the case of *Federal Republic of Nigeria v Chief Emmanuel Nwude & Ors*.[8] The accused in this case, was alleged to have carried out the third world biggest single scam with numerous others pending in count. In consequence, the accused persons were charged to the High Court of Lagos State on a 57 count charge, including obtaining money by false presences, to the tune of US $181.6 million and they were all found guilty and sentenced accordingly. In addition to this sentence, their assets were forfeited to the Federal Government of Nigeria and the sums of money recovered were returned to their owners. Sections 14 – 18 stipulate offences within the remit of the Act. This includes offences in relation to

[1] Extradition Act Cap. E25, Laws of the Federation of Nigeria, 2004
[2] *Ibid*, Section 1.
[3] Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 52.
[4] *Ibid*, Section 53.
[5] Evidence Act 2011.
[6] Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 57.
[7] O. Ehimen and A. Bola, 'Cybercrime in Nigeria' (2010) 3(1) *Business Intelligence Journal* 95.
[8] Suit No: CA/245/05

 

financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to economic and financial crimes.

Section 46 of the Act defines 'economic crime' as the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either-individually or in a group or organised manner, thereby violating existing legislation governing the economic activities of government and its administration. It includes any form of fraud, narcotic drug tra cking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human tra cking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse dumping of toxic wastes are prohibited.

Section 7(2) of the EFCC Commission (Establishment) Act 2004, equips the Commission with the responsibility of enforcing the provision of:-

a) The Money Laundering Act 2004
b) The Advance Fee Fraud and Other Related Offences Act 2006
c) The Failed Banks (Recovery of debts) and Financial Malpractices in Banks Act 1994, as amended.
d) The Banks and Other Financial Institution Act 1991 (Reenacted 2020)
e) Miscellaneous Offences Act
f) Any other law or regulations relating to economic and financial crimes including the Criminal Code or Penal Code.

It is submitted that the EFCC (Establishment) Act 2004, empowers the EFCC to investigate and prosecute perpetrators of cybercrimes (Internet or online advance fee fraud in Nigeria) while placing reliance on the Advance Fee Fraud and other related offences Act 2006 and other relevant legislations. For instance in *Harrison Odiawa v. Federal Republic of Nigeria,*[1] the accused person who impersonated one Abu Belgore was arraigned by the EFCC on a 58-Count charge of offences, including conspiracy to obtain by false pretense, obtaining by false pretense, forgery, uttering and possession of documents containing false pretense contrary to the Advanced Fee Fraud and Other Related Offences Act. In the course of the trial, the prosecution testified that a solicitation e-mail was sent to one Mr. George Robert Blick (the nominal complainant), an American citizen resident in Virginia, USA by the accused and his cohorts seeking a foreign contractor to facilitate the transfer of $20.5 million US dollar. In the said mail, he was asked to respond if he was interested and Mr. George did by e-mail stating that he had a United States registered corporation that could be used to receive the said funds. For the purposes of documentation and finalization of the contract, the accused and his cohorts demanded for several sums of money from the accused through exchange of e-mails, telephone conversations and fax ranging from 187, 000 US dollars (creation of new documents), 10,000 pounds (opening of bank account), 18,750 US dollars (trust processing fee), 410,000 US dollars (payment for issuance of ICP number), 750,000 US dollars (resolution of petition against the transaction), 250,000 US dollars (for Nigerian Minister of Finance before ICP number can be issued), 350,000 US dollars (for newly appointed Nigerian Minister of Finance), 300, 000 Euros (for transportation), 1.5 million US dollars (for the repair of damaged part of machine), 1.2million dollars (for insurance of machine), which Mr. George obliged them. Thereafter, communications between the parties ceased and then it dawn on Mr. George that he had been defrauded. He consequently wrote a petition to the EFCC, which led to the arrest of the accused. At the conclusion of hearing, Hon. Justice J.O.K. Oyewole held 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 obtain the various sum of money contained in counts 2,8,10,12,14,18,20,22,24 and 28 from him and found the accused guilty as charged. Dissatisfied with the judgment of the court, the accused appealed to the Court of Appeal. The Court of Appeal dismissed the appeal and affirmed the judgment and conviction and sentences of the trial court.

From the aforementioned provisions, it can be clearly seen that though the EFCC Act effectively deals with internet related fraud, the Act still does not go a long way in dealing with cybercrimes. This is because internet related fraud is only a piece of the puzzle. Cybercrime encompasses internet-related fraud and involves other crimes such as hacking, cyber-stalking, child pornography among other crimes.

### 4.2 Advanced Fee Fraud and Other Fraud Related Offences Act

The Advanced Fee Fraud and Other Related Offences Act[2] was enacted to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences and to repeal other Acts related therewith. Advance fee fraud is a vexing threat and a major problem in Nigeria today.[3] The Act provides for ways to combat cybercrime and other related online frauds.

The Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretense, use of premises, fraudulent invitation, laundering of fund obtained through unlawful

[1] (2008) All FWLR (Pt. 439) 436.
[2] Advanced Fee Fraud and other Fraud Related Offences Act 2006, CAP A6, LFN 2010
[3] M. Chawki, 'Nigeria Tackles Advance Fee Fraud' (2009) 1 *Journal of Information, Law & Technology* 4.

 

activity, conspiracy and aiding among other crimes. Section 2 makes it an offence to commit fraud by false pretense. This section can be used to prosecute criminals who commit cybercrimes like computer related fraud, where the offender uses an automation and software tools to mask the criminal's identities, while using the large trove of information on the internet to commit fraud. According to Section 7, a person who conducts or attempts to conduct a financial transaction involving the proceeds of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity; or where the transaction is designed to conceal or disguise the nature, location, source, ownership or control of proceeds of a specified unlawful activity, he is liable on conviction to a fine of ₦1 million and in the case of a director, secretary or other o cer of a financial institution or corporate body or any other person, to imprisonment for a term, not more than 10 years and not less than five years.

In the case of *Mike Amadi v. Federal Republic of Nigeria,*[1] the Appellant (Mike Amadi) was charged before the High Court of Lagos State by the EFCC *inter alia* with attempt to obtain the sum of US$125,000.00 (One Hundred and Twenty Five Thousand United States Dollars) from one Fabian Fajans by sending fake e-mails through his mail box and registered websites in respect of a forged Central Bank of Nigeria payment schedule containing false pretense by requesting for money to process the transfer of Two Million, Five Hundred Thousand United State Dollars ($2.5 million USD) being the contract sum for the generators Fabio Fajans was purported to have supplied the Federal Government of Nigeria for the All African Games 2003 and by falsely representing to Fabio Fajans that the said sum of US$125,000.00 represent the five percent (5) processing fees of the total sum of USD 2.5 million contrary to sections 5(1), 8(b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act. On 20 May 2005, the High Court found him guilty and sentenced him to 16 years imprisonment. Aggrieved with the judgment of the High Court, the Appellant appealed to the Court of Appeal. The Court of Appeal affirmed the judgment of the High Court. On further appeal to the Supreme Court, the Supreme Court while dismissing the appellant's appeal, the judgment and sentences of the High Court and the Court of Appeal were affirmed.

The Act also made certain provisions by imposing duties on electronic communications service providers such as telecommunications service providers, Internet service providers and owners of telephone and Internet cafes for the purpose of intercepting or halting the use of the Internet and telecommunications facilities in the perpetration of advance fee scam. For instance, the Act obliges any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form to obtain full names, residential address, in the case of an individual; corporate address, in the case of corporate bodies) from customer or subscriber.[2] Any customer or subscriber who fails to furnish the required information or with the intent to deceive, supplies false information or conceals or disguises the required information commits an offence and is liable on conviction to imprisonment for a term of not less three years or a fine of N100,00.[3] Section 12(3) in addition to the above penalty makes service providers to forfeit the equipment or facility used in providing the service.

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 Economic and Financial Crimes Commission; 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.[4] Similarly, anyone whose normal course of business involves the provision of a non-fixed line or Global System of Mobile Communication(GSM), or is in the management of any such services is mandated to submit on demand to the EFCC any data or information necessary or expedient for giving effect to the enforcement of the Advance Fee Fraud and Other Related Offences Act by the EFCC.[5] By virtue of section 13(3) of the Act, telecommunications and service providers owe a duty of care to ensure that their services and facilities are not utilized for unlawful activities. Failure on the part of electronic communications service providers to comply with the aforementioned duties results commission of an offence and is liable on conviction to imprisonment for a term of not less than three years without an option of fine and in the case of a continuing offence, a fine of ₦50,000 for each day the offence persists.[6]

In *Nnachi Ephraim v. Federal Republic of Nigeria*,[7] the Court of Appeal explained the purport of Section 13. Here, the Appellant was convicted at the Federal High Court Kaduna pursuant to the charges of operating Prime Gate Cyber café at No. 1 Abakiliki, carrying out Internet and Telecommunications services contrary to the

[1] (2008) 12 SC (Pt.III) 55.
[2] Advanced Fee Fraud and other Fraud Related Offences Act 2006, Section 12(1).
[3] *Ibid*, Section 12(2).
[4] *Ibid*, Section 13(1)(a) & (b).
[5] *Ibid*, Section 13 (2).
[6] *Ibid*, Section 13 (5).
[7] (2012) LPELR – 22363(CA).

 

provisions of section 13(1)(a) and punishable under section 13(5)(c) of the Advance Fee Fraud and Other Related Offences Act 2006. Aggrieved by the judgment of the Federal High Court, the Appellant appealed before the Court of Appeal Kaduna. The Court of Appeal, while setting aside the conviction and sentence of the Appellant held per Orji-Abadua, JCA on the offence of non-registration of cybercafé – when a person can be said to have committed an offence under section 13(1)(a) of the Advance Fee Fraud and Other Related Offences Act 2006, as follows:

> For a person to be guilty under section 13(1)(a), the person must in the normal course of business, provide telecommunications or internet services, or must be the owner or the person in the management of any premises being used as a telephone or Internet café or whatever name called. I must observe that the fact that the signboard of Prime gate cybercafé is posted at No. 1 Okpara Street, Abakiliki notwithstanding, there must be some act on the part of the owner of the cybercafé to prove that he actually provides telecommunications or internet services to the public. There was no shred of evidence adduced by the prosecution establishing that Prime gate Cybercafe was indeed providing telecommunications and Internet services at No. 1 Okpara Street Abakiliki…There must be proof of the usage of the place as a telephone or internet café. This was lacking in the evidence proffered by the prosecution in the instant case.[1]

### 4.3 Money Laundering (Prohibition) Act

Another related law regulating internet scam is the Money Laundering (Prohibition) Act 2004.[2] It makes provisions to prohibit the laundering of the proceeds of crime or an illegal act. Section 14(1)(a) of the Act prohibits the concealing or disguising of the illicit origin of resources or property which are the proceeds of illicit drugs, narcotics or any other crime. Sections 17 and 18 of the Act also implicate any person, corporate or individual, who aids or abet illicit disguises of criminal proceeds. Section 10 mandates financial institutions to make compulsory disclosure to National Drugs Law Enforcement Agency (NDLEA) in certain situations prescribed by the Act.

In the same way, if it appears that a customer may not be acting on his own account, the financial institution shall seek from him, by all reasonable means, information as to the true identity of the principal. This enables authorities to monitor and detect suspicious cash transactions and these sections can be used against criminals who use the internet as a means of unlawfully transferring large amounts of money from one account to another.

### 4.4 Criminal Code

The Criminal Code Act[3] was enacted to establish a code of criminal law in Nigeria. The criminal code criminalizes and sanctions any type of stealing of funds, in whatever form and false pretenses. Although, cybercrime is not specifically mentioned in the Act, crimes such as betting, theft and false pretenses performed through the aid of computers and computer networks are types of crime punishable under the Criminal Code Act. Sections 239(2)(a) and 240A of the Criminal Code Act prohibit betting and public lotteries, respectively. Section 239(2)(a) provides that any house, room or place used for the purpose of any money or other property, being paid or received therein by or on behalf of such owner, occupier, or keeper or person using the place as or for an assurance, undertaking, promise, or agreement, express or implied, to pay or give thereafter any money or other property on any event or contingency of or relating to any horse race or other fight, game, sport or exercise, of any house, room, or place knowingly and willfully permits it to be opened, kept or used or any person who has the use or management of such business of a common betting house is guilty and liable to imprisonment for one year, and to a fine of one thousand Naira. This section can be used by law enforcement agencies to regulate "Online Betting' or prosecute such persons as would contravene the section.

Section 418 defines false pretense as 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 to be true. Cybercrime that would fall under this section would mainly bother on computer related fraud. By their fraudulent action, cybercriminals deceive their victims by pretending to have abilities or skills they ordinarily do not have or possess. Most activities of these cyber criminals bother on false pretenses and cheating, which sections 419 and 421 of this Act prohibit respectively. Section 419 states that 'any person who by any false pretense, and with the 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 a felony and is liable to imprisonment for three years'. Furthermore, a suspect could be charged under section 421 of the Act which provides that any person who by means of any fraudulent trick or device 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 or to pay or deliver to any person any money or goods, or any greater sum of money or greater

[1] *Ibid*.
[2] Money Laundering (Prohibition) Act Cap M18, LFN 2010.
[3] Criminal Code Act, Cap 38, LFN 2010.

 

quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour, and is liable to imprisonment for two years. A person found committing the offence may be arrested without warrant.

Unfortunately, the Criminal Code is a British legacy, which predates the internet era and understandably does not specifically address email scams.[1] For example, notwithstanding that section 419 of the Criminal Code criminalizes computer-related fraud, the position that a suspect cannot be arrested without a warrant, unless found committing the offence, does not reflect the mode of perpetrating the crime in the cyberspace.[2] Only in exceptional circumstances could a suspect be caught in the act, especially with the advancement of technology in the information world of today. Furthermore, aside from the fact that Nigeria lacks the resources to police activities of Nigerians on cyberspace, doing so could actually raise privacy or other rights issues.[3] Also, the punishment for an internet fraudster which is three years imprisonment or seven years if the value of stolen property exceeds one thousand naira is to say the least paltry compared to the enormity of the crime and unjust rewards that usually run into millions of dollars. Moreover, in criminal trials, the state is the complainant and under the Nigerian criminal justice system, there is hardly any form of compensation for the victims of the crime.

## 5. Cybercrime Prevention in other Jurisdiction

### 5.1 The United States of America

Given the federal system of government in the United States of America, laws concerning computer crimes are enacted at the state and federal levels.[4] In 1986, Congress passed the Computer Fraud and Abuse Act (CFAA), 1986. This law has been amended and expanded as internet technology advanced, and it continues to form the basis for federal prosecutions of computer related criminal activities.[5]

The Act makes obtaining financial or credit information through a computer a crime. Before the Act was put in place, there was not much that could be done for computer fraud in the United State of America. Not only did this Act help fight against computer fraud, but it also acted against the use of computers as a means of inflicting damage on other computing systems.[6] The Computer Fraud and Abuse Act (CFAA)[7] makes it illegal for anyone to distribute computer code or place it in the stream of commerce if they intend to cause either damage or economic loss. The Act focuses on a codes damage to computer systems and the attendant economic losses, and it provides criminal penalties for either knowingly or recklessly releasing a computer virus into computers used in interstate commerce. Someone convicted under the Computer Fraud and Abuse Act could face a prison sentence of 20 years and a fine of up to $250,000.[8] Hence, the development and possession of harmful computer code would not amount to a criminal act, however using the code can amount to a criminal act. Each major subsection of the Computer Fraud and Abuse Act is intended to explain a particular aspect of computer crime. In simple terms, the Computer Fraud and Abuse Act prohibits:

a) accessing a computer without authorization and subsequently transmitting classified government information;[9]
b) theft of financial information;[10]
c) accessing a "protected computer";[11]
d) computer fraud;[12]
e) transmitting code that causes damage to a computer system;[13]
f) trafficking in computer passwords for the purpose of affecting interstate commerce or a government computer[14] and
g) computer extortion.[15]

One of the most prominent events in the history of computer crime in America was the terrorist attack of September 11, 2001. Though this attack was not directly related to computer crime, it led to the enactment of the

---

1 Chawki, above (n 71)
2 T. Oriola, 'Advance Fee Fraud on the Internet' (2005) 21 *Computer Law and Security Report* 241.
3 F. E. Eboibi 'Curtailing Cybercrime in Nigeria: Applicable Laws and Derivable Sources' (2017) 2 *AFJCLJ* 14.
4 S. W. Brenner, 'State Cybercrime Legislation in the United States of America: A Survey' (2001) 7 *Rich. J.L. & Tech.* 28.
5 S. Eltringham, 'Prosecuting Computer Crimes', Computer Crime and Intellectual Property section, Office of Legal Education, Executive Office for United States Attorneys, available at: https://www.justice.gov/criminal/file/442156/download accessed 11 March 2022.
6 C. Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service 2014) 1.
7 Computer Fraud and Abuse Act 1986, 18 U.S.C. Section 1030.
8 CFAA 1986, 18 U.S.C., Section 1030(c).
9 Section 1030(a) (1).
10 *Ibid*, Section 1030(a) (2).
11 *Ibid*, Section 1030(a) (3).
12 *Ibid*, Section 1030(a) (4).
13 *Ibid*, Section 1030(a) (5).
14 *Ibid*, Section 1030(a) (6).
15 *Ibid*, Section 1030(a) (7).

 

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA PATRIOT Act) 2001. This Act gave government agencies an increased ability to crack down on computer crime in the name of intercepting and obstructing terrorism.[1]

The National Information Infrastructure Protection Act 1996, which was signed into law by then-President Clinton in 1996, significantly amended the Computer Fraud and Abuse Act 1986. Its definition of a "protected computer" was expanded to effectively cover any computer connected to the internet.[2] It criminalizes the use of government computers to obtain confidential records such as an individual tax or medical record. Violators are to be charged with the crime of using computer to disperse sensitive document.[3] Furthermore, the Act increased the penalties for offences created in Computer Fraud and Abuse Act 1986.

### 5.2 The United Kingdom

The Computer Misuse Act 1990 (CMA ) was introduced in August 1990 following a Law Commission report surrounding computer misuse which found that the UK was trailing behind many EU member states in relation to technological development.[4] The Act makes provision for securing computer materials against unauthorised access or modification; and for connected purposes. It introduced three new offences into the U.K criminal law, these are:

a) unauthorized access to computer material;[5]
b) unauthorized access with intent to commit a further offence;[6]
c) Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer.[7]

The basic notion of hacking whereby an individual causes a computer to perform a function when at the time he intends to access a program or data held in a computer, is covered by the offence of unauthorized access to computer material.[8] The ingredient of this offence is simply an access to computer material without authorized and knowledge of the lack of authority to access the material.[9] No intention is required for this crime to be committed; so long as there has been unauthorized access with the knowledge of not being authorized the crime has taken place. On what amount to 'not being authorized', section 17(5) of the Computer Misuse Act 1990 offers some guidance by specifying that, if the defendant was not entitled to access of the kind in question and had no consent to, then entry is unauthorized.[10] In *Ellis v. DPP (No. 1)*[11] the legal question in issue was whether an ex-student's use of a log-in terminal, knowing he was prohibited could be "unauthorized" use under section 1. Lord Woolf CJ held that the access was still unauthorized, and that the statutory provisions were sufficiently wide enough to include the use made of the computers by the appellant. Also in the case of *R v. Bow Street Magistrates and Allison*,[12] House of Lords held that insider hackers would be liable under section 1 of the Computer Misuse Act 1990 where the employer clearly defined the limits of the employee's authority to access programmes or data and such employee exceed the limit.

Section 2 of the Act[13] provides for the penalty of unauthorized access to computer material with the intent to commit or facilitate the commission of further offences. The basic notion is that someone guilty of an offence under section 1 of the Act[14] will have further criminal sanctions imposed on him if this is done with the intention to commit or facilitate the commission of further offences. 'Further offences' under section 2 are those which have a sentence fixed by law or where an individual found guilty of that offence would be liable for a term of imprisonment of five years or more.[15]

It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.[16] A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.[17] Section 3 of Computer Misuse Act 1990 was amended by the Police and Justice Act, 2006. Its aim was to tackle

1 USA PATRIOT Act 2001, Explanatory Memorandum.
2 National Information Infrastructure Protection Act 1996, Section 201.
3 *Ibid*, Section 201.
4 N. Macewan, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future' (2008) *Criminal Law Review* 955.
5 Computer Misuse Act 1990, Section 1.
6 *Ibid*, Section 2.
7 *Ibid*, Section 3.
8 *Ibid*, Section 1.
9 *Ibid*.
10 *Ibid*, Section 17(5).
11 [2001] EWHC Admin 362.
12 [2000] 2 A.C. 216.
13 Computer Misuse Act 1990.
14 *Ibid*.
15 *Ibid*.
16 *Ibid*, Section 2(3).
17 *Ibid*, Section 2(4).

 

computer viruses and denial of service attacks, which can have devastating effects on the organizations targeted. The offence does not have to be against a particular computer, program or data and is committed even if, for example, the denial of service is only temporary.[1]

Subsequently, the Serious Crime Act, 2015, added a new offence of "unauthorized acts causing, or creating risk of, serious damage".[2] A person is guilty of an offence of 'unauthorized acts causing, or creating risk of, serious damage' if: (a) the person does any unauthorised act in relation to a computer; (b) at the time of doing the act the person knows that it is unauthorised; (c) the act causes, or creates a significant risk of, serious damage of a material kind; and (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.[3]

Damage is of a "material kind" for the purposes of this offence if it is: (a) damage to human welfare in any place; (b) damage to the environment of any place; (c) damage to the economy of any country; or (d) damage to the national security of any country.[4] The territorial scope of computer misuse was also extended, meaning that a UK national is still committing an offence if the computer misuse happened outside the UK, as long as it was also illegal in the country where the hacking took place.[5]

Penalties for offences under the Computer Misuse Act 1990 range from two years imprisonment and/or a fine for unauthorized access to computer material; up to five years and/or a fine for unauthorized access with intent to commit or facilitate commission of further offences; up to 10 years and/or a fine for unauthorized modification of computer material; and imprisonment for life and/or a fine for breach of section 3ZA.

The Computer Misuse Act 1990 has been amended to make sure that hackers that launch serious attacks, such as those on critical infrastructure could face life imprisonment.[6]

## 6. Effectiveness of the Cybercrimes (Prohibition, Prevention etc) Act 2015 and other Ancillary Laws

The Cybercrimes (Prohibition, Prevention Etc.) Act 2015 addresses the most important aspects of cybercrimes and even extended beyond. The Act is a well-articulated effort to discourage some behavioural activities within the cyberspace by outright legislative proscription. For example, behavioural patterns such as cyber stalking, cybersquatting, computer-related fraud and forgery, cyber terrorism and the likes, are prohibited and violations attract a wide range of sanctions, including monetary fines and terms of imprisonment under the Act. The highlight of the offences and penalties is one aspect that gives the Act a credit, what matter the most now is the crucial aspects of the implementation and enforcement of the Act. A lackluster attitude to the enforcement may defeat the purpose of the Act. On the other hand, successful enforcement may only be achieved if it avoids harassment, abuse of privacy, abuse of office, and extortion of genuine users of the internet. Enforcement however, must be characterized by the desire to achieve accountability, sincerity, rigor and steadfastness in the implementation and administration of the Act for its effective use.

As at yet, there is no convicted case based on the Cybercrimes (Prohibition, Prevention Etc.) Act 2015, however, there are few cases still in trial on the enforcement of the Act. One of such cases is the *Economic and Financial Crimes Commission v. Azeez Fashola* (*Naira Marley)*.[7] The accused was charged with 11 counts charges of offenses bordering on internet fraud. According to the EFCC, the defendant committed the offences on different dates between November 26, 2018, and December 11, 2018, as well as May 10, 2019. The Commission alleged that Fashola and his accomplices conspired to use different Access Bank ATM cards to defraud their victims. It also alleged that the accused had in his possession counterfeit credit cards belonging to different people, with intent to defraud which amounted to theft. The anti-graft agency said the offences, contravened the provisions of sections 23(1) (b), 27(1) and 33(9) of Cyber Crime (Prohibition, Prevention etc) Act, 2015.

At the resumed sitting on 27th of February 2021, the prosecution through its second prosecution witness (PW2), Augustine Anosike, an investigator and forensic expert with the EFCC, sought to tender in evidence a compact disc (CD) containing information, analysis and extractions from the defendant's phone. During his evidence at the previous sitting, Mr. Anosike had told the court that the forensic analysis that was carried out on Naira Marley's iPhone revealed some shocking evidence against him. He said the evidences were extracted and burnt into a CD, alongside some documents that were printed out.

The judge adjourned the matter for admissibility of documents brought before the court in evidence against the accused. We believe that the court will finally give judgement in this case for the first time under the new Cybercrime (Prohibition, Prevention etc) Act 2015. However, without prejudice to the effectiveness of this Act,

[1] The Police and Justice Act 2006, chapter 48 in force on October 1st 2008.
[2] The Computer Misuse Act 1990, Section 3ZA.
[3] Serious Crime Act 2015; the Computer Misuse Act 1990, Section 3ZA.
[4] *Ibid*.
[5] The Serious Crime Act 2015; The Computer Misuse Act 1990
[6] O. Solon, 'U.K Law Introduces Life Sentence for Cyber Criminals' (2014), <http://www.wired.co.uk/article/cybercrime-bill-life-sentence > accessed 11 August 2021.
[7] The case filed at the Federal High Court has suit number FHC/L/178c/19.

 

the scourge of cybercrime unabated. In fact, the crime has taken new dimensions and sophistication. This is attributed to the rising culture of 'get rich quick' syndrome in Nigeria and lack of global census in tackling the menace of cybercrime. One of the greatest impediments against global efforts towards stemming the whirlwind of cybercrimes remains the anonymous nature of the identity of cybercriminals. The unfettered freedom of information and communication enables the cybercriminals to hide their identity using different telecommunications gadgets so as to make it impossible to trace the online Internet Protocol (IP) address of any user. A good example is the use of VPN, Psiphon, The Onion Router (Tor) etc. Furthermore, if the IP address of a cybercriminal were traced to a particular location, the next hurdle cannot be scaled as the identity of a cybercriminal is undisclosed to the owner or operator of Internet service provider.[1]

## 7. Recommendation and Conclusion

There is no doubt that cybercrime has taken a great toll on global trade and economic activities. As the use of the internet has grown astronomically, so has the efforts of unscrupulous elements doubled to defraud unsuspecting users in the cyberspace. The scourge of cybercrime affects individuals, businesses and countries and as such, it is a great threat to the economic and financial sanctity of nations, which explains why all countries prohibit the menace. Nigeria in a bid to tackle cybercrime has enacted the Cybercrimes (Prohibition, Prevention etc) Act 2015 and other sundry legislations to tackle the increasing penetration of cybercrimes in the country. This paper examined the Nigerian Cybercrimes Act and these legislations dealing with cybercrimes in Nigeria. Despite the novel provisions of the Cybercrimes Act, the paper found that it has not reduced substantially the rate of cybercrime in the country. In view of the low patronage of Act in stemming cybercrimes in Nigeria, the paper makes the following recommendations:

a) The Nigerian public should be enlightened on how exactly computer systems and computer data can be protected. For example, the use of anti-viruses and passwords among the public should be encouraged. There are cases where the infiltration of a computer system is disguised to look as if it came from a source that is absolutely unaware of the breach. This is made possible because of lack of comprehensive security such as firewall, passwords and anti-viruses on the victim's network. The use of anti-viruses and passwords among the public would go a long way in enhancing computer security.
b) Although Section 8 of the Cybercrime Act deals with unauthorized modification of computer data, which definitely include the use of computer viruses to modify computer systems and data, it does not cover the ambit of creation and distribution of computer viruses. Section 8 of the Act should be widened to effectively deal with the creation and distribution of computer viruses so as to help enhance computer security and combat cybercrime.
c) Furthermore, section 15 of the Cybercrime Act, which provides for cyber stalking should be extended to email spam that is, sending large amount of unsolicited commercial emails.
d) Section 24(3) of the Cybercrime Act providing for the training of law enforcement agencies should be extended to cover judges in the training so as to aid the effective implementation of the Act.
e) The Cybercrime Advisory Council established under Section 25 of the Cybercrime Act should be made to go through a periodic training relating to combating of cybercrime, so as to enable them to get the latest development relating to cybercrime and the methods of fighting it. This is pertinent, because the nature of cybercrime and the methods by which it can be effectively prevented and prosecuted are very dynamic.
f) The Cybercrime Act should provide for compensatory damages and other form of relief to victims who suffer from acts of cybercriminals, just as it is provided for in the American jurisdiction, under section 1030(g) of the Computer Fraud and Abuse Act.
g) Since the level of unemployment in the country has contributed significantly to the spate of cybercrime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where the youths can come together and display their skills. This can be used meaningfully towards developing IT in Nigeria and job creation strategy.

## References

Ajayi, E. F. G. 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6(1) *Journal of Internet and Information Systems* 1.

Ashaolu, D. 'Combating Cybercrimes in Nigeria' in D. Ashaolu, (ed.) *Basic Concepts in Cyberlaw* (Velma Publishers, 2012)

Brenner, S. W. 'State Cybercrime Legislation in the United States of America: A Survey' (2001) 7 *Rich. J.L. & Tech.* 28.

[1] E. F. G. Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6(1) *Journal of Internet and Information Systems* 1-12.

 

Chawki, M. 'Nigeria Tackles Advance Fee Fraud' (2009) 1 *Journal of Information, Law & Technology* 4.
Chukkol, K.S. *The Law of Crimes in Nigeria* (Revised Edition, Ahmadu Bello University Press Ltd, 2010).
Clemente, D. *Cyber Security and Global Interdependence: What Is Critical?* (Chatham House, Royal Institute of International Affairs 2013).
DataReportal, 'Digital 2022: Global Overview Report', available at: https://datareportal.com/reports/digital-2022-global-overview-report accessed 11 March 2022.
Doyle, C. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service 2014) 1.
Eboibi, F. E. 'Curtailing Cybercrime in Nigeria: Applicable Laws and Derivable Sources' (2017) 2 *AFJCLJ* 14.
Ehimen, O. and Bola, A. 'Cybercrime in Nigeria' (2010) 3(1) *Business Intelligence Journal* 95.
Ekhator, E.G. 'A Study of Electronic Signature and Its Legal Validity in Nigeria' (2020) 1 (1) *Lawrit Student Journal of Law* 47.
Eltringham, S. 'Prosecuting Computer Crimes', Computer Crime and Intellectual Property section, Office of Legal Education, Executive Office for United States Attorneys, available at: https://www.justice.gov/criminal/file/442156/download accessed 11 March 2022.
Furnell, S. *Cybercrime: Vandalizing the Information Society* (London: Addison-Wesley 2002) 21; T. Jordan, & P. Taylor, 'A Sociology of Hackers' (1998) 46 *The Sociological Review* 757–780.
Grabosky, P.N. 'Virtual Criminality: Old wine in New Bottles?' (2001) 10 *Social and Legal Studies* 243–249.
Hollinger, R.C. & Lanza-Kaduce, L. 'The Process of Criminalization: The Case of Computer Crime laws' (1988) 26 *Criminology* 101–126.
Holt, T.J. and Bossler, A.M. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses* (Routledge 2016).
International Telecommunication Union (ITU) 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) September Report, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html accessed 14 July 2021.
Izuakor, C.F. 'Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context', *ISSA Journal,* 2021, 28-29.
Kshetri, N. 'Pattern of Global Cyber War and Crime: A Conceptual Framework' (2005) 11(4) *Journal of International Management* 541.
Macewan, N. 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future' (2008) *Criminal Law Review* 955.
Nigerian Communication Commission, 'Final Report on: Effects of Cybercrime on Foreign Direct Investment and National Development,' 15 https://www.ncc.gov.ng/documents/735-nmis-effectscybercrime-foreign-direct-investment/file accessed 11 August 2021.
Okeshola, F. and Adeta, A. 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria Kaduna State, Nigeria' (2013) 3(9) *American Journal of Contemporary Research* 98
Olayemi, O. 'A Socio-Technological Analysis of Cybercrime and Cyber security in Nigeria' (2014) 6(3) *Academic Journal* 116.
Olowu**,** D. 'Cybercrimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa' (2009) 1 *Journal of Information, Law and Technology*.
Olusola,M.'Cyber Crimes and Cyber Laws'(2013) 2(4) *The International Journal of Engineering and Science* 19.
Oriola, T. 'Advance Fee Fraud on the Internet' (2005) 21 *Computer Law and Security Report* 241.
Parker, D.B. *Crime by Computer* (Charles Scribner's Sons 1976).
Solon**,** O. **'**U.K Law Introduces Life Sentence for Cyber Criminals' (2014), <http://www.wired.co.uk/article/cybercrime-bill-life-sentence > accessed 11 August 2021.
Statista, 'Number of Internet Users in Nigeria from 2017 to 2026', available at: https://www.statista.com/statistics/183849/internet-users-nigeria/ accessed 14 March 2022.
Wall, D.S. 'Digital Realism and the Governance of Spam as Cybercrime' (2004) 10 *European Journal on Criminal Policy and Research* 309–335.
Yusuf, M. O. 'Information and Communication Technology and Education: Analysing the Nigerian National Policy for Information Technology' (2005) 6(3) *International Education Journal* 316-321.
Zahri, Y., Ahmad, R. and Yusoff, M. 'Grounding the Component of Cyber Terrorism Framework Using the Grounded Theory' (2014) *Science and Information Conference* 523-529.
*Economic and Financial Crimes Commission v. Azeez Fashola* (*Naira Marley)* FHC/L/178c/19.
*Federal Republic of Nigeria v Chief Emmanuel Nwude & Ors*. Suit No: CA/245/05
*Federal Republic of Nigeria v Osahon* (2006) 5 NWLR (Pt. 973) 361.
*Harrison Odiawa v. Federal Republic of Nigeria* (2008) All FWLR (Pt. 439) 436.
*Mike Amadi v. Federal Republic of Nigeria* (2008) 12 SC (Pt.III) 55.
*Nnachi Ephraim v. Federal Republic of Nigeria*, (2012) LPELR – 22363(CA)