KSUJPL Volume 7, 2022 ISSN: 2141-4300

KOGI STATE UNIVERSITY JOURNAL OF PUBLIC LAW

JOURNAL OF PUBLIC LAW

CONTENTS

Competence of the Child Witness: Illuminating the Provisions of the Evidence Act, 2011
SE Kabo, PhD 1-18

The Evolving Practice of Plea Bargaining in Criminal Cases in Nigeria
Prof. Alili Ngozi, Ph.D and *Friday O Ogwo* 19-32

The Enforcement of the Convention on the Rights of the Child and its Optional Protocol on Armed Conflicts Against Child Soldering: Potentials and Limits
Obinna Nnanna Okereke 33-54

Open Grazing Prohibition Legislations in Nigeria: A Panacea for Conflict and Insecurity
Caroline Mbafan Ekpendu, PhD 55-67

Legal Framework for the Prohibition of Child Abuse in Nigeria
Adeyemi Oluwadamilare (Mrs) and
Adeyemi Olutosin Babajide 68-89

Historical Perspective of Corporate Income Regulations and Fiscal Policy Matters in Nigeria
Ademola A Taiwo, PhD, Adesoji Adebayo and
Emmanuel Chinaka 90-101

Ensuring an Operational Equity-Based Nigerian Refugee Law: Overcoming The Legal and Regulatory Constraint
Nnawulezi Uche, Ph.D and *Ogbusu Victoria* 102-128

Conceptions and Misconceptions about the Roles of Next of Kin, Administrators and Executors in the Management and Control of The Estate of A Deceased Person under The Law
Omodele Adeyemi Oyedele 129-140

Challenges in the Enforcement of Cybercrimes Law in Nigeria: Yahoo Plus as Case Study

*Shuaib Oniye**
*Prof. Abiodunamuda-Kannike***

Abstract

Information technology has made the world a global village and has enhanced every sector of the society. The innovation in computer, information communication and internet, cuts across every sectors in Nigeria because our society is becoming an information society where communication takes place in cyberspace. Thus, the society is threatened by the growing tread of cybercrime which has created avenue for miscreants to engage in cyber criminality against cyber citizens, and in order to curb the menace of cybercrime, the Nigeria government enacted Cybercrimes (Prohibition & Prevention) Act 2015 with aim to provide an effective, unified, and comprehensive legal, regulatory & institutional framework for prohibition, prevention, detection, prosecution and punishment of cybercrimes offenders in Nigeria. However, despite this, in the list of the many sustainability challenges facing Nigeria as a country today, internet fraud comfortably enjoys a top position, because internet fraudsters have attained a higher dimensions known as yahoo plus, connote using spiritual power to defraud unaware cyber citizens. To this end, this paper, while adopting analytical research methodology, examines the challenges in the enforcement of cybercrime law in Nigeria using Yahoo plus practitioners as a case study.

Key words: Enforcement, Cybercrime, Law, Yahoo Plus, and Nigeria.

---

* Dept.of Jurisprudence and Public Law, Faculty of Law, Kwara State University Malete, Kwara State. Sub4law@gmail.com +23407037377554.

** SAN, Dean Faculty of Law, Kwara State University Malete, Kwara State. +23408033256756: +23409072388483: info@amudakannikesan.com : amudakannikeabiodun@gmail.com.

1.1 Introduction

The advent of Information technology has made the world a global village wherein the international communities have access to the world from their homes, office, cyber cafes and so on which has enhanced every sphere and sector of the society like economy, commerce, social religion, and educational sectors[1]. Despite its advantages, the society is however threatened by the growing trend of cybercrime, where a computer is either used as a tool or target or it involves elements of information technology infrastructure[2].

Cybercrime has been observed as one of the most challenging and dynamic security threats of this generation and may creep into the next without sufficient cyber criminological data and studies[3].The crime has resulted to a lot of havoc to corporate organizations, cyber citizens, governments across the globe. Its attributes amongst others are seen in: adverse reduction of competitive strength of corporate organizations; unnecessary time wasting and sluggish economic/ financial growth, it enhances money laundering; it encourages fraud on social media; it is a danger to international security.[4]

In international communities, cybercrime occupy an important and increasingly strategic role and has reflected in the formation of major international bodies and various treaties, convention, and bilateral, regional and international agreements across nations of the world[5]. Many cyber citizens have been victims of this crime, it is believed that individual youth want to live a very comfortable life without necessarily engaging in physical work; invariably defrauding others through the internet claiming that their activities such as online

---

1 Maitanmi O& others, 'Cyber Crimes and Cyber Laws in Nigeria' *The International Journal Of Engineering And Science (IJES)* Volume 2 Issue 4 (2013) Pages 19-25

2 Ibid

3 A Olayinka. & R.S Babajide, 'Yahoo-plus in Ibadan: Meaning, Characterization and Strategies'[2020](13)*International Journal of Cyber Criminology*344.

4 A.B Hassan and J Makinde, 'Cybercrime in Nigeria: Causes, Effects and the Way Out' [2012](7) *ARPN Journal of Technology Science and Technology*,629.

5 N Kshetri, 'Cybercrime and cyber security in the global south' [2013] Hampshire: Palgrave Macmilla.

romance scam, E-commerce fraud, consumer scam, advance fee fraud[6] bit coin and online gift card are legit. The issue of crime related to cyber has raised series of fundamental questions among stakeholders in Nigeria[7].The offence can be committed against individual, property and government, because online payments cut across all industries and are being used by a significant elite individuals in each sectors[8], yet this crime continues to be on the increase despite effort on the part of the government to minimise its rising among Nigerian youth.

It is against this background that this paper examines the challenges in the enforcement of cybercrime law in Nigeria with particular emphasis on the activities of Yahoo plus practitioners with a view to making necessary recommendations.

2.1 Theoretical Framework

Scholars across the globe have attempted to define cybercrime based on their understanding of the concept without unanimous agreed definition. For instance, the Black's Law Dictionary defines cybercrime as a crime involving the use of computer, such as sabotaging or stealing electronically stored data[9].According to the Council of Europe (COE) Convention on Cybercrime, cyber-crime involves "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data[10]. the Federal

---

6 F E Eboibi, 'Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence' (2011) *Nigerian Law and Practice Journal*, 140.

7 O Tolulope, 'Youth Perception on Yahoo-Yahoo (Cybercrime): A Case Study of Ado-Ekiti, Ekiti State Nigeria' Degree of Masters in Criminology and Forensic Studies in the Faculty of Humanities, School of Applied Human Sciences, University of Kwazulu Natal, Howard College, Durban, South Africa. 2017

8 Ibid

9 *Black's Law Dictionary* 7th edition

10 Council of Europe (COE) Convention on cybercrime Retrieved from <http://conventions.coe.int/Treaty/en/Treaties/ html/185.htm> (2001) accessed on 25th day of June, 2021

Bureau of Investigations[11] (FBI), opined that cybercrimes spans across a diverse scenario including; crimes against children (usually involving child pornography or child rape); theft of intellectual properties and/or publications, phishing, intentional dissemination of malware to national and international internet fraud[12].

Similarly, Thomas and Loader in their view described cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks[13]". It encompasses all illegal activities perpetrated by one or more people referred to as scammers, hackers, internet fraudsters, yahoo boys, using the internet through the medium of networked computers, telephones and other information and communications technology (ICT) equipment.

Historically, cybercrime is gradually advances as technology develops. In 1960, cybercrime focused on physical destruction of computer system parts and stored data[14]. In the mid-1960s, the United States criminal abuse focused on databases and the related risks to privacy[15]. In 1970s, traditional ways of committing crimes such as manual stealing was in place; however the innovation of computer modernized ways of stealing. In 1980s, the number of computer systems increased, hence creating more potential targets for Cybercrimes.[16]Early 1990s, World Wide Web (www) was introduced and this led to a tremendous growth in the number of Internet users, and this invention also welcomed new challenges in the cyber world.

---

11 Federal Bureau of Investigation. Press release: Internet fraud investigation operation cyber loss. <http://www.fbi.gov/pressrel/pressre l01/ifcc052301.htm> (2001) accessed on 25th day of June, 2021

12 Ibid

13 D Thomas, &B Loader, 'Introduction to Cybercrime: Law Enforcement, Security and Surveillance in The Information Age' (London: Routledge. 2000).

14 Tanebaum, Regarding network protocols, Computer Networks; Come Technology (JILT), <http://go.warwick.ac.uk/jilt/2009_1/chawki> (2001) accessed on 5th day of June, 2021

15 F B Okeshola & A.K Adeta, 'The Nature, Causes and Consequences of Cyber-Crime in Tertiary Institutions in Zaria-Kaduna State [2013] 3(9) Nigeria' *American International Journal of Contemporary Research* 98-114.

16 Ibid

It means more advanced functions, more perpetrators and more hackers were active within the cyber space[17].

In Nigeria, the story of cybercrime and the rise of the Yahoo boys are strongly related with the introduction of the Internet. The first Internet[18] connection to Nigeria was installed in 1995 through the UNESCO-sponsored Regional Informatics Networks for Africa. At the dawn of the forth era of democratization in Nigeria in 1999, internet access through mobile phones dominated the society with roughly 350 000 users,[19]During this time, an internet corporation named Yahoo, which provided multiple services such as email and search engines, was the global market leader[20]. Yahoo maintained its dominance as a service provider for years in Nigeria which led to the name being used as slang to refer to the internet[21]. Since internet was popularly referred as yahoo at point of introducing the service to Nigeria youth that engaged in activities relating to the internet were immediately labelled "yahoo-yahoo" boys[22]. This practice is popular among Nigerian youths and involves defrauding foreigners as well as Nigerians to the tune of millions of dollars annually[23]. For example, they execute this crime by way of using fake identities on dating websites such as elite' singles, match.com, bit coin, gift card etc. this is how the introduction of information technology which gradually aids our day to day activities and at the same time being one of the most challenging and dynamic security threats of this generation.

Cybercrime is a crime that uses information technology and is one form transnational crime does not recognize borderless, without violence, there is no physical contact and without name that makes Cyber Crime actors very difficult to traced and the necessary elements of cybercrime criminal elements are difficult to established,

---

17 A.B Hassan and J Makinde(n 4)

18 The Internet is "a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols" (Oxford University Press, 2013).

19 Tolulope Ojolo (n9)

20 Ibid

21 Ibid

22 A Doppelmayr, 'It's All About Love: Organization, Knowledge Sharing and Innovation Among the Nigerian Yahoo Boys' (Master's thesis). 2013)

23 Ibid

likewise the statute of limitation to give locus standi[24]. Protection of victims of cybercrime requires seriousness and high expertise from law enforcement agency i.e. legal officers and police prosecutors who are saddled with responsibility to apprehend and prosecute cyber criminals[25]. It is therefore necessary to consider the reaction and responses of the international communities, regional and at national level to the security threat posed by cybercrime to the cyber citizen and the general public across the globe.

3.0 Legal Instruments on Cybercrime

Cybercrime is a crime that cuts across national borders, is not limited to one jurisdiction, it's without violence, and no physical contact is required to commit the offence. An extra-territorial jurisdiction principle approach is necessary and requires cooperation between all related elements, nationally, regionally and internationally. The one regional which serve as international Convention[26] on Cyber Crime was formed with considerations, among others: First, that the international community is aware of the need for cooperation between countries and industries in combating cybercrime and the need to protect legitimate interests in the use and development of information technology. Second, conventions are currently needed to reduce the misuse of systems, networks and computer data to commit criminal acts. Its main focus is to deal with infringements of copyright, child pornography, computer related fraud and violations of network security. And such problems are dealt by Convention by providing the common perception on cybercrimes, authentication of cyber-crime acts, jurisdiction and international co-operation in dealing with it.The only binding international instrument against cybercrime nowadays is ECC. It serves as a guideline for any country

---

24 R W Massulthan & A Ridwan'Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?[2020] (5)(1) IJCLS *Indonesian Journal Of Criminal Law* Studies<http://journal.unnes.ac.id/sju/index/php/ijcls> 63-74 accessed on 8th August, 2021.

25 Ibid

26 Convention on Cyber Crime initiated by the European Union came into effect on June 2001. Along with the Council of Europe the Convention was signed by US, Canada and Japan. It has been also ratified and accessed by 41 countries and 11 countries signed without following with ratification.

developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties.

Article 2 Convention provides that each Party shall adopt such legislative and other measures as may be necessary as criminal offences under its domestic law, intentionally, the access to the whole or any part of a computer system without right[27]. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intentions, or in relation to a computer system that is connected to another computer system. Article 3 of the Cybercrime Convention, reads: each Party shall adopt such as legislative and other measures as may be necessary to establish as criminal offense under its domestic law, intentionally, the interception without right, made by technical means, from non-public transmissions of computer data to, from within a computer system, including electromagnetic emissions from a computer system carrying such computer data[28].It covers type of cybercrime such as illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights[29]

At regional level, the African Union (AU) at her 23rd session of the summit of the AU in Malabo, Equatorial Guinea adopted the AU Convention on Cyber security and Personal Data Protection, wherein member states were urged to adopt legal measures to curb cybercrime.[30] However, Article 36 of the convention requires signature/ratifications of at least 15 member's states before the convention is enforceable; this clause has not been achieved till date which serves as impediment to the impact of the convention among African states.

Due to increase of internet fraud, which has generated an upsurge of reprehensible acts; that such criminality require the response of a

---

27 Ibid Article 2
28 Ibid Article 3
29 Ibid Article 4-11
30 African Union Convention on Cyber Security and Personal Data Protection, Art. 25

legal regime and a suitable punishment because of the level of damage they generate, the Economic Community of West African States (ECOWAS) at her sixty-sixth ordinary session of the council of ministers issued a directive on fighting cybercrime within ECOWAS States and urged member states to adopt necessary legislative, regulatory and administrative measures to enforce it.[31]The directive in its article 1 defined cybercrime article 2 aims and objective of the member states geared towards adapting a substantive criminal law to address the menace of cybercrime.[32] Article 3 contains the scope of the Directive, basically applicable to all cyber-related offence within the ECOWAS sub-region.[33]Others provides for offences such as fraudulent access to computer systems; fraudulently remaining in a computer system; interfering with the operation of a computer system; fraudulent input of data in a computer system; fraudulent interception of computer data; fraudulent modification of computer data; computer data forgery; obtaining benefit from computer related fraud; fraudulent manipulation of personal data; use of forged data; obtaining equipment to commit an offence; participation in an association or agreement to commit computer offence; production of child pornography or pornographic representation; import or export of child pornography or pornographic representation; possession of child pornography or pornographic representation; facilitation of access of minors to pornography, documents, sound or pornographic representation; possession of racist or xenophobic written documents or pictures through a computer system; threat through a computer system; abuse through a computer system; denying or justifying acts or crimes against humanity by means of a computer system; aggravating circumstances of common law offences; violations of computer data, software and programme[34] etc.

---

31 ECOWAS sixty-sixth ordinary session of the council of ministers Directive C/DIR. 1/08/11 on fighting cybercrime within ECOWAS; preambles 10-13; Art. 35

32 Ibid Art.2

33 Ibid Art.3

34 Ibid. Art. 4-25

The Nigeria government with her unrelenting efforts has enacted several laws on cybercrime and other related offences[35] and at the same time established law Enforcement Agencies to curb the menace of cybercrimes in the country. Noticeable among various laws is the Advance Fee Fraud and Other Related Offences Act 2006, which repealed the Advance Fee Fraud and Other Related Offences Decree No. 13 of 1995.The Act prohibits cybercrime and other related online frauds such as; obtaining property by false pretence,[36] use of premises for fraudulent activities, fraudulent invitation, laundering of funds obtained through unlawful activity, attempts, conspiracy, aiding and abetting, amongst others. According to Section 23[37]'False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' the Act also made certain provisions by imposing duties on electronic communications service providers such as telecommunications service providers, 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.[38]

In a bid to put in place stronger legal framework to curb cybercrime, a revision of the existing cybercrime legislation was put forward by the Nigeria Government and in May 2015, the cybercrime bill was signed into law, properly defining the act as unlawful with penalties attached to any disobedience of the law. The Act[39]is the first specific

---

35 Among the laws are Nigeria Criminal Code Act 1990, Constitution of the Federal Republic of Nigeria, 1999 (as amended), Nigerian Communications Act 2003, Economic and Financial Crimes Commission (Establishment) (EFCC) Act 2004, Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006, National Information Technology Development Agency (NITDA) Act 2007, Evidence Act 2011, Money Laundering (Prohibition) (Amendment) Act, 2012, Cybercrimes (Prevention, Prohibition Etc) Act 2015.

36 Nigerian Advance Fee Fraud and Other Related Offences Act, 2006, section 1 & 2. The Nigerian Supreme Court have had course to entertain an online Advance Fee Fraud case; Mike Amadivs Federal Republic of Nigeria (2008) 12 SC (pt.III) 55 brought by EFCC for obtaining money by false pretence.

37 The Advance Fee Fraud Act (Laws of the Federation of Nigeria, 2006).

38 Ibid section 13 (1).

39 Cybercrimes (Prevention, Prohibition) Act 2015

law that creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters. Specifically, the Act engenders a platform for cyber security and in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information. Section 1 contains the objectives of the Act; section 2 provides that the provisions of this Act shall apply throughout the Federal Republic of Nigeria. The Act define Offences such as Unlawful access to a computer, System Interference, Interception of Electronic messages, e-mails, electronic money transfer, Tampering with critical infrastructure, Wilful misdirection of electronic messages, Unlawful interceptions, Computer, related forgery, Computer related fraud, Theft of electronic devices, Unauthorised modification of computer systems, network data and system interference, Cyber-terrorism, Fraudulent issuance of e-instructions, Identity theft and impersonation, Child pornography and related offences, Cyber stalking, Cyber-squatting, Racists and xenophobic offences, Importation and fabrication of e-tools, Breach of confidence by service providers, Manipulation of ATM/POS terminals, Phishing, spamming, spreading of computer virus[40] etc. Recourse will be made to the provisions of this Act being the famous among other laws on internet fraud and cybercrimes related offences later when discussing the activities of yahoo plus.

Other laws on internet fraud and cybercrime related offences are the Constitution of the Federal republic of Nigeria, 1999 (as amended) in it's section 37 provides for right to privacy, homes correspondence, telephone conversations and telegraphic communications.[41] It guarantees privacy right which is against cybercrime, illegal computer hacking or online stalking by private person or group[42]. Again, section 7 (2) of the EFCC Commission (Establishment) Act 2004, equipped the Commission with the responsibility of enforcing the provision of the following laws: The Money Laundering Act

---

40 Ibid section 10-36.

41 Constitution of the Federal Republic of Nigeria, 1999(as amended) Section 37

42 F Eboibi, 'Curtailing Cybercrime in Nigeria: Applicable Laws and Derivable Sources'[2017] (2) *AFJCLJ* 1-19.

2004;The Advance Fee Fraud and Other Related Offences Act 2006; The Failed Banks (Recovery of debts) and Financial Malpractices in Banks Act 1994, as amended;· The Banks and Other Financial Institution Act 1991, as amended; Miscellaneous offences Act f) Any other law or regulations relating to economic and financial crimes including the criminal code or penal code[43]. Similarly, the Criminal Code Act of 1990[44]has similar provision regarding internet fraud and other cybercrimes related offences. The Act in its section 418 defined what constitutes an offence under the Act, when it state that any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence[45]. While section 419 states: Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years[46]. It is therefore necessary to state at this point that there are adequate laws governing cybercrimes and internet fraud both at regional and national level. What then is the response of these laws to the activities of the internet fraudster particularly yahoo plus scenarios in Nigeria.

4.1 Yahoo Plus Activities

Cybercriminals popularly known as yahoo boys in Nigeria use various methods in getting their victims across the planet into fraudulent scams via spam mails, cash-laundering e-mails, cyber

---

43 Economic and Financial Crimes Commission (Establishment) Act 2004): *Harrison Odiawa v Federal Republic of Nigeria* [2008] All FWLR (pt.439) 436 where the accused person who impersonated to be Abu Belgore was arraigned by the EFCC on 58 Count of offences; Conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering and possession of documents containing false pretence contrary to the Advanced Fee Fraud and Other Related Offences Act. It was held that from the evidence adduced by the prosecution, it is evident that the accused and his cohorts had a common intention to defraud their victim.

44 The Criminal Code Act, Cap C38 LFN 2004.

45 Ibid section 418

46 Ibid section 419

cafes, Identity theft and impersonation,[47] Child pornography, Cyber stalking, Cyber-squatting, Racists and xenophobic offences, Importation and fabrication of e-tools, Breach of confidence by service providers, Manipulation of ATM/POS terminals, Phishing, spamming, spreading of computer virus browsing the internet all night, sending scam mails to unsuspecting victims pretending to be female to defraud cyber citizens. These would be explain edhereunder as follow:

4.1.1 Cyber Terrorist

A cyber-terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them.[48]Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website, email server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Section 18 (1) of the Act provides that "any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment[49]. In order to further strengthen the fight against terrorism, EFCC signed MOU[50] when the chairman of the commission said: INTERPOL provides a wide range of policing expertise and capabilities, supporting three main crime programmes: Counter-terrorism, Cybercrime, Organized and Emerging Crimes. The commission are mobilising for the enlistment of all law enforcement agencies in Nigeria, and consider to kick start the assignment at the EFCC.

---

47 Cybercrimes Act, (n39) section 22.

48 Maitanmi Olusola & others (n 1)

49 Cybercrimes Act (n39) section 18

50 The Economic and Financial Crimes Commission, EFCC, on November 29, 2018 signed a Memorandum of Understanding, MoU, with the International Police, INTERPOL as part of collaboration aimed at tackling corruption in Nigeria. The MoU, according to chairman of the commission Magu, will further create a greater technical team work and allow the EFCC to be connected to the 194 member countries of the organisation. <www.efcc.ov.ng> accessed on 15th day of August, 2021

4.1.2 Cyber Stalking

This refers to using the Internet to repeatedly harass another person, it could be sexual in nature including cursing anger because People usually leave a lot of information about themselves online unprotected. It encompasses intentionally sending of mails via computer system that is grossly offensive or pornographic, to annoy, inconvenience, obstruct, insult, cause criminal intimidation to another.[51] This is punishable upon conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than three (3) years or to both[52]. In the case of *Harrison Odiawa v Federal Republic of Nigeria*[53] the evidence before the court was that the accused person sent solicitation e-mail under false pretence to his victim. It was held that it is evident that the accused and his cohorts had a common intention to defraud their victim and found the accused guilty as charged thereon having proved her case beyond reasonable doubt.[54] Also, in *Mike Amadi v Federal Republic of Nigeria*[55] where the Appellant was charged before the High Court of Lagos State Holden at Ikeja by EFCC for sending fake e-mails through his mail box princemike2001@yahoo.comrequesting money under false pretence. He was convicted and sentenced to 16 years imprisonment.[56]

4.1.3 Spreading Of Viruses

Viruses such as Trojans, worms, malware and other software that gets onto your computer without your knowledge.[57] The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. In some cases a piece of malware will pretend to be a legitimate piece of software, when such software is downloaded, it infects the computer system and destroys valuable information/data store on it. It is an offence which attract three (3) years imprisonment if found guilty. The

---

51 (n39) section 24
52 Ibid
53 [2008] All FWLR (pt.439) 436
54 Ibid
55 [2008] 12 SC (pt.III) 55
56 Ibid
57 Maitanmi Olusola & Others (n1)

section says: any person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers shall be guilty of an offence is liable upon conviction to three (3) years imprisonment or a fine of N1,000,000.00 or both[58]

4.1.4 Cyber Squatting

This involves intentional use of a name, business name, trade mark, domain name or other word or phrase registered, aimed or in use by any individual, body corporate or belonging to either the Federal, State or Local Government in Nigeria, on the Internet or any other computer network without authority or right and for the purpose of interfering with their use by the owner. The act is punishable and Liable on conviction to imprisonment for a term of not more than two (2) years or a fine of not more than five million naira N5,000,000.00 or to both fine and imprisonment.[59] See the case of FRN v John Padre Akor[60] the defendant was charged under Section 33(5)[61] , with intent to defraud one John Smith of the United States of America, obtained control over a card as security for debt and thereby committed an offence. The defendant was sentenced to three (3) years imprisonment with an option of fine of N1.5million.

4.1.5 Phishing/Spamming

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. For instance, internet fraudster who hacked into a financial institution account sent an email asking the target victim to verify personal information through a link to a fraudulent

---

58 (n39) section 32 (3)

59 (n39) section 24 (1)

60 *FRN v John Padre Akor* (unreported) before Justice Abdu Dogo of the Federal High Court sitting in Makurdi, Benue State on Thursday July 8, 2021<www.efcc.gov.ng> accessed on 15th day of August, 2021.

61 Cybercrimes Act (n39) section 33 (5)

web page. Once that is provided, the hacker can access the victim's financial information and transfer money instantly. Section 32 of the Act provides that any person who engages in Phishing and spamming with intent to disrupt the operations of a computer be it public or private or financial institutions shall be guilty of an offence and liable upon conviction to 3 years imprisonment or a fine of ₦1, 000,000.00 or both.[62]

4.1.6 Fraud Identity Theft

This could range from a black-hat hacker stealing online banking account login and password to getting access to automatic teller machine (ATM) and using such people can make themselves a lot of money with personal information. Fraud identity is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone and pretending to be somebody else with the aim of cheating the victim. section 22 (1) says any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud is guilty of an offence and upon conviction shall be sentenced to 7 years imprisonment or N5, 000,000.00 fine or both. In the unreported case of FRN v Mbanugo Ifeanyi[63] the defendant was arraigned on charges bordering on forgery, impersonation and obtaining money from unsuspecting foreign nationals under false pretences. The defendant pleaded guilty to the charged as read, he was convicted and sentenced to two (2) years imprisonment with an option of One Million Naira fine.[64] Similarly in FRN v Adeyemi Opeyemi Joshua (a.k.a Godeaux Ellis Spencer) and ors[65] the defendants were arraigned on separate

---

62 (n39) section 32 (1) & (2)

63 *FRN v Mbanugo Ifeanyi* (unreported) before Justice I.M Buba of the Federal High Court sitting in Enugu on Tuesday July 6, 2021 www.efcc.gov.ng accessed on 15t day of August, 2021

64 Ibid

65 *FRN v Adeyemi Opeyemi Joshua* (a.k.a Godeaux Ellis Spencer) and ors (unreported) the defendants were arraigned on Friday June 25, 2021 before Justice Uche Agomoh of the Federal High Court sitting in Ibadan, on separate one count charge for offences bordering on fraudulent impersonation contrary to Section 22 (2) (a) and 22 (2) (b) of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

one count charge for offences bordering on fraudulent impersonation contrary to Section 22 (2) (a) and 22 (2) (b) of the Act. They pleaded "guilty" to the charges. The court convicts the defendants and sentenced them to six months imprisonment each. The court also orders that the defendants should forfeit all the items recovered from them to the Federal Government of Nigeria.[66]

Cyber criminals in Nigeria while defrauding cyber citizens through any of the above means as highlighted employed the aids of spiritual power term yahoo plus. Yahoo plus means using different forms of spiritual means to enable them carry out this crime. It is generally believed that the ordinary yahoo is no longer yielding huge sums of money, hence, the need to upgrade.[67] This is why yahoo plus is often regarded as a higher or upgraded version of "yahoo yahoo."Yahoo plus is an advanced form of yahoo yahoo whereby the "yahoo boys" employs traditional spiritual means like voodoo or juju to hypnotize their victims into doing their bidding and parting with whatever amount of money they request for.[68] The yahoo boys indulge in occultist ritual practices to enhance their potential to defraud people. There are various strategies deployed in achieving this feat. The yahoo boy approaches a spiritualist or diviner who consults, the "oracle" or the "gods" Once this is successfully done, the victim is guaranteed to keep remitting money from wherever he or she is in the world.[69]This is evident when the victims send a huge amount of money that an ordinary or reasonable man acting reasonably wouldn't have agree to. To buttress this point, in the case of FRN v Adeyemi Opeyemi Joshua (a.k.a Godeaux Ellis Spencer) and ors (supra) the court held *inter alia* that the defendant should pay the sum of $650 (Six Hundred and Fifty United States Dollars to victim of his

---

66 Ibid

67 O A Samuel, and others, 'Yahoo Boys Phenomenon in Lagos Metropolis: A Qualitative Investigation' [2019] (13) (1) *International Journal of Cyber Criminology*

68 Ibid

69 O S Adesina, 'Cybercrime and Poverty in Nigeria' [2017] (13) (4), *Journal of Canadian Social Science* 19-29. Available from: http://www.cscanada.net/index.php/css/article/view/9394 DOI: <http://dx.doi.org/10.3968/9394>

fraud, and forfeit one Samsung S8 Duos Mobile phone and an IPhone X to the Federal Government.

In dealing with the use of spiritual power to defraud unsuspecting victims, section 210 (1) (c) of Criminal Code Act[70] which provides that "any person who makes or sells or assist or take part in making or selling or using or has in his possession or represents himself to be in possession of any juju, drug or charm which is intended to be use or reported to possess the power to prevent or delay any person from doing an act which such person has a legal right to do, or to compel any person to do an act which such person has a legal right to refrain from doing ... is liable to imprisonment for two years."

Again, section 217 of penal code[71] provides that "whoever knowingly has in his possession any fetish or charm which is pretended or reputed to possess power to protect a person in the committing of any offence shall be punished with imprisonment which may extend to five years or with fine or with both."

From the combined meaning and interpretation of the sections cited above, the test to be use in determining when yahoo boys employ any fetish or charm to defraud the targeted victims (called yahoo plus) is that of reasonable man, i.e. whether an ordinary or reasonable man acting reasonably would have agree and consent to transfer huge amount of money without any legal transaction between the sender and the recipient. This was the scenario in FRN v Joseph Oladapo Philips[72] the defendant (Philips) who is an undergraduate of the Sokoto State University was prosecuted for dishonestly representing himself as an American soldier serving in Afghanistan and obtaining the huge sum of $18,700 by false pretence. The defendant was convicted and sentenced to 10 years imprisonment.[73]The convict was

---

70 Criminal Code Act Cap C38 Laws of Federation of Nigeria 2004: Also, section 213 of the Act on criminal charm or fetish act which attracts five years imprisonment upon conviction.

71 Penal Code (Federal Provision)Act, Cap P3 Laws of the Federation of Nigeria 2004.

72 *FRN v Joseph Oladapo Philips* (unreported) before Justice Mohammed Sifawa of the Sokoto State High Court on Friday, July 23, 2021. www.efcc.gov.ng accessed on 12th day of August, 2021

73 Ibid

also ordered to pay the sum of $18,700 United States Dollars as restitution to the victim through the EFCC.

5.1 Challenges of Enforcement of Prohibition of Criminal Acts of Yahoo Boys

It is obvious there are increases in young boy's involvement in internet fraud in Nigeria. It appears that there are two major reasons; the first is the combination of unemployment and poverty. While second is peer group influence[74], even though both are untenable excuse in law. There are challenges facing law enforcement Agency in their quest to protect online businesses and efforts being made against cyber criminals. One of such is jurisdiction which has exacerbated the rate of cybercrime in Nigeria. The cyber criminals can sit in the confine of their room and commit a crime that will affect another who resides in other jurisdiction. Jurisdiction is so radical that it forms the basis of any adjudication and goes into the roots of any matter before the courts. If a court lacks jurisdiction, it also lacks the necessary competence to try the case.[75]The question is whether it can be said that cybercrime offences lack *locus delicti* or whether the offences could be said to have more than one *locus delicti* because the cases are multi-jurisdictional. Thus, extradition is seen as an option of solving the jurisdiction challenge, but there must be an existence of extradition treaty between states to automatically return cybercriminals for trial.[76] And in such case, the dual criminality principle needs to be fulfilled. This simply means that before a suspect can be validly extradited, both the requested state and state of domicile of the criminal must ensure that the alleged offence is punishable in their respective states. In Nigeria, both Federal High Court[77] and state high court[78] have jurisdiction to try offences involving internet fraud. Another factor that hinders the enforcement of cybercrime law is that young people that are under the age of eighteen are mostly involved. By virtue of juvenile law

---

74 O Tolulope (n7)

75 *Dairo v. Union Bank of Nigeria Plc* [2007] 16 NWLR (pt 1059) 99

76 Extradition Act, Cap E 25 Laws of the Federation of Nigeria, 2004 Section 1 and 2.

77 Cybercrimes Act (n39) section 52

78 If the offender is to be charged under the Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006

they enjoy protection because they are regarded as infants.[79] Thus even when they are caught, the law does not punish but rehabilitate and reintegrate them into the society because they are consider as fresh tree that is amendable.[80] This is evident from several cases cited earlier, despite the conviction and sentences, the defendants were given option of fine so as to avoid incarceration.

Again, lack of trained Personnel equipped with adequate model facilities is one of the reasons why the fight against cyber criminals is cumbersome to actualise. It would be very difficult for investigating officer to detects fraud if he/she is not well trained and acquit himself with tactics being used in the cyber would. More so, our financial institutions both government and private owned are still lack perquisite knowledge to counter internet fraud being perpetrate by cyber criminals. When customer money is fraudulently transferred (may be to buy recharge card), sometimes it would be difficult if not impossible for the bank to trace the money, making the customer to lose the money completely too online fraudster. Corruption has also play a vital role because it has enhanced the growth of Internet crime in Nigeria. When these cyber criminals are caught and being investigated, bribe may be offered or demanded and it encourages other youths to perpetrate online fraud.

6.0 Conclusion and Recommendations

The impact of the information communication technology especially with regards to online transactions cannot be over emphasized. However, some persons with criminal intent have also taken advantage of these developments to perpetrate cybercrime against cybercitizens. It has increased level of youth involvement in cybercrime which is major concern to the world. This ugly trend has affected virtually all sectors of the society and is negatively affecting the image of this country. This paper analyse the various legal instrument both regional and at national level enacted by Nigeria government to tackle internet fraudster, examine several ways of conducting cybercrime by fraudster such as cyber terrorism, malware,

---

79 Umejiaku N.O. and Anyaegbu M.I, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria' [2016] (15) (10) *International Journal of Computer and Technology* 1-10.

80 Ibid

cyber stalking, spam/phishing, fraud identity theft etc. against cyber citizen. Internet fraudsters (yahoo boys) while engaging in any of these practices, employed the use of criminal charms, fetish, to defraud unsuspecting cyber citizens. It is, however, not clear how prosecutors are able to provide and justify evidence of fetishism and ritual practices against the suspect in the court of law. The paper highlighted challenges which hinder enforcement of cybercrimes law in Nigeria.

The paper observed that with the commencement of Cybercrimes (Prevention, Prohibition) Act 2015, Nigeria has now joined nations with comprehensive law to investigate and prosecute cybercriminals. Fighting cybercrime requires a holistic approach to curb this menace in all ramifications. The government, stakeholders, financial institutions and every member of the society should ensure that web page are fully secured to avoid being hijack by fraudsters, need to keep up with technological/security advancement and exercise duty of care towards other Internet users. The Nigeria's government should provide enabling environment and ensure adequate security to online businesses in order to minimise if not eradicate hijack of internet transactions by fraudster and equipped our law enforcement Agency with necessary updated weapons/facilities to detect and prosecute cybercrime offenders accordingly in order to ensure that Nigeria preserves or enhances its economy and social stability of the country.