ANALYSIS OF THE LEGAL AND INSTITUTIONAL FRAMEWORK FOR FIGHTING CYBERCRIME IN NIGERIA*

Abstract

The internet has become an integral part of life today. Its role to economic development and communications cannot be overemphasized. It can be said that the World is now capable of doing a lot of things which were unimaginable decades ago. The internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance on the machines. Internet has made life easier to mankind with just a click on a computing devise one can get what they want from the internet anytime and anywhere irrespective of geographical boundaries. With all the benefits accruing to the use of the internet, the emergence of cybercrime has brought serious threats to people and States. There have been a lot of efforts made by Nigerian governments, police departments and intelligence units against the threat caused by cybercrime. In a concerted effort to fight cybercrime, the Nigerian government enacted the 2015 Cybercrime Act. This article will attempt to analyse the legal and institutional framework for cyber-crime in Nigeria while revealing the challenges faced by the regulatory agencies in the fight against cybercrime. It is expedient to also know that the article adopted the doctrinal method of research through legal preposition, doctrines, laws and legal concept of research. The work recommends that the information technology professionals will find it very helpful if involved at the investigation level as consultants to law enforcement agencies. By way of conclusion, the need to set up an independent regulatory body with the sole responsibility of controlling cybercrime in Nigeria cannot be overemphasized.

Keywords: Cybercrimes, Law, Regulatory Agencies, Judiciary, Nigeria

1. Introduction

Cybercrime and its vices such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing[1] are under the jurisdiction of the Economic and Financial Crimes Commission (EFCC) and EFCC is the body empowered by government to fight all forms of financial crimes including cyber-crimes in Nigeria and they are working together with the cyber-crime prevention working group. Therefore, EFCC is charged with the responsibility of investigating and prosecution of all economic and financial crimes.[2] However Nigeria has legislative laws such as the Nigeria Criminal Code Act 2004 which is established to regulate crimes generally in Nigeria,[3] but the National Assembly as the legislative body must as a matter of urgency amend certain sections of the Criminal Code to address cybercrimes because the act of cybercrimes increase every day.[4] The researcher is of the view that though the EFCC deals with financial and economic crimes, it is the Criminal Code that has all powers to deal effectively with cybercrimes. As a result of the nature of cybercrimes and an undeveloped national legal framework on cybercrimes, cybercrimes often occur internationally.[5] Cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries, as Professor James Boyle noted, 'if the King's writ reaches only as far as the king's sword, then much of the content on the internet might be presumed to be free from the regulation of any particular sovereign,'[6] this observation is particularly pertinent in the criminal enforcement context and it is impossible to regulate criminal behavior without a means to ensure enforcement of sanctions.[7] The jurisdictional problem of cybercrime manifests itself in three ways: (i) lack of criminal statutes; (ii) lack of procedural powers; (iii) lack of enforceable mutual assistance provisions with foreign states.[8] However the aim of this chapter is to analyse the legal

***By Iyadah John VIKO, LLM, MSc, PhD (Aberdeen, United Kingdom), Lecturer,** Faculty of Law, Nasarawa State, University Keffi. Email-vikoiyadah@gmail.com; vikoiyadah@nsuk.edu.ng. Phone No: 08035970989.

[1] E, Adebimpe, 'Cybercrime in Nigeria: Detection and Prevention,' (2016)1 *Journal of Engineering and Technology* p.37.
[2] O. Sam, 'Cybercrimes and Cyber Laws in Nigeria' (2016) 2*International Journal of Engineering and Science,* p. 22.
[3]Criminal Code Act 2004.
[4] ibid.
[5]M. Keyser, 'The Council of Europe Convention on Cybercrime' (2003) 12, *Journal of Transnational Law and Policy*, p.288.
[6] M. Amalie, 'The Council of Europe's Convention on Cybercrime,' (2003) 18 *Berkeley Technology Law Journal* p. 425.
[7] Ibid.
[8] Ibid.

regulatory framework of cybercrime prevention in Nigeria and to examine whether there is a regulatory agency designed for curbing cybercrime in Nigeria and the majors put in place to control cybercrimes in Nigeria and how effective these majors are.

2. Analysis of the Legal Framework for Cybercrime in Nigeria

This section provides an overview of legal measures to the phenomenon of cybercrime by explaining legal approaches in criminalizing certain acts. Criminal Law provisions covering the most common forms of computer crimes can today be found in a large number of countries, the situation with regard to digital evidence is different. Only a few countries have so far addressed specific aspects of digital evidence and, in addition, international binding standards are lacking.[9] This section provides the legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. Cross border activities on the internet do not respect geographical limits, and as a result of illegal conduct or transactions, particularly in the field of internet commerce, the parties are subject in many cases to a wide array of laws and regulations, and often contradictory claims with regards to the interpretation of the laws and jurisprudence where the parties reside and where the transaction took place.[10] The solutions to resolve conflict of laws issues and determine aspects of applicable law and jurisdiction for cross border transactions among private parties are usually achieved through the application of private international law.[11] In countries with civil law systems like Nigeria, jurisdictional aspects targeting the fields of cyber space has not specifically been addressed due to the judicial systems tradition to strictly follow and interpret legislation contained in written codes and regulations.[12] Hence as its inflexibility to follow and adapt foreign rules and precedents on jurisdiction in cyber space.[13] Furthermore, the academic doctrine and literature in this particular field of law has just started to be developed.[14] As identified in the previous section domestic laws on its own cannot effectively address the problem of cybercrime, a need for international coordination of laws and binding treaty agreements between countries (bilateral or multilateral) is timely due to the transnational nature of cyber-crime because various countries have established treaty agreements in place while other countries are still struggling to adopt domestic Penal Law, however harmonization is necessary for both substantive and procedural laws.[15] All countries have to reappraise and revise rules of evidence, search and seizure, electronic spying etc, to cover digitized information in order to conform to modern computer and communication systems, and the global nature of the internet. Better coordination of procedural laws, therefore, would facilitate cooperation in investigations that cover multiple jurisdictions.[16]

Legislations Regulating Cybercrimes in Nigeria

Effective legislation can be said to be one of the major steps in controlling cybercrime. In 2004, the Nigerian government established the Nigerian Cybercrime Working Group comprising representatives from government and the private sector to develop legislation on cybercrime, furthermore, in 2007, the government established the Directorate for Cyber Security (DfC), which is an agency responsible for responding to security issues associated with growing usage of internet and other information and communication technologies (ICTs) in the country.[17]Apart from these initiatives, there are general laws that are not specifically related to cybercrime but are being enforced to deal with the crime and some of these laws, which will be examined below, are: 1999 Constitution of the Federal Republic of Nigeria, Criminal code Act (1990), Penal code 2009, 2011 Evidence Act (As amended), Money Laundering (prohibiting) Act 2011, Economic and Financial Crimes Commission (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006, Computer Security and Critical Information Infrastructure Protection Bill, 2005 Cybercrime (Prohibiting, Prevention etc) 2015.

[9] G. Marco,'Understanding Cybercrime: Phenomena, Challenges and Legal Response,' (2012) 1 *International Telecommunication,* Union Publisher Geneva, p.169.
[10] A. Laura, 'Cyber Crime and National Security: The Role of the Penal Code and Procedural Law' (2011) 2 *Law and Security in Nigeria* 222.
[11] ibid.
[12] ibid.
[13] ibid.
[14] ibid.
[15] Ibid.
[16] Ibid.
[17]A. Olubukola, 'Cyber Crime and Poverty in Nigeria,' (2017)13/4 *Canadian Social Science* 25.

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The first point of call for cybercrime protection under the Nigeria legal jurisprudence is the 1999 Constitution of the Federal Republic of Nigeria (as amended), Section 37 of the Constitution provides that the privacy of citizens, their homes, correspondence telephones conversations and telegraphic communication is hereby guaranteed and protected.[18] According to the Constitution, the individual's right to privacy is sacrosanct and it can only be fettered by laws made by democratically enabled public authorities in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or for the protection of the rights and freedom of others.[19] In the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting rights and freedom of other persons assume from the above, the right to privacy of an individual even when protected by the constitution can be compromised by any act of the federation which seeks to protect public safety, order and interest thus, enforcement of the right of privacy, under the constitution may not be readily obtainable: an individual may need to seek redress under other applicable laws.[20]

Economic and Financial Crime Commission (Establishment) Act 2004

This Act was enacted to repeal the Financial Crimes Commission (Establishment) Act, 2002. Section 1 of the Act establishes a body known as the economic and financial crimes commission (EFCC), the Act provide the legal framework for the establishment of the Commission. Some of the major responsibilities of the commission are provided for in part 2 of the article of the Economic and Financial Crime Commission Establishment Act 2004. Part two of the Act listed out the responsibilities of the commission which are the investigation of financial crimes which include advance fee fraud, money laundry, and counterfeiting illegal charge transfers, future market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, among other responsibilities as listed in the Act.[21] However this part covers a lot of computer related crimes and it can be helpful in the regulation of cybercrime in Nigeria. Economic crime is defined as 'the non-violent criminal and illicit activity committed with the object of earning wealth illegally, either individual or in group or organized manner thereby violating legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking, and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including countering of currency, theft of intellectual property and open market abuse, dumping of toxic waste and prohibited goods.'[22] Section 5 of the EFCC Act has been the basis for various actions of EFCC including their actions in the case of Emmanuel Nwude (the accused) in *Federal Republic of Nigeria v. Chief Emmanuel Nwude & Ors*[23]. Which the accused were charged to court on a 57-count charge and they were guilty and sentence accordingly. 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 problem. Cybercrime encompasses internet-related fraud and involves other crimes such as hacking, cyber-stalking, child pornography among other crimes.

Computer Security and Critical Information Infrastructure Protection Bill 2005

In 2005, the Nigerian government adopted the Computer Security and Critical Information Infrastructure Protection Bill (known as the Cybercrime Bill).[24] The Bill aims to secure computer

[18] 1999 Constitution of the Federal Republic of Nigeria (as amended).
[19] O, Umejiaku, M. Anyaegbe, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria,' (2010) *Nnamdi Azikwe University Journal* 16.
[20] ibid.
[21] Economic and Financial Crime Commission (Establishment) Act 2004.
[22] O. Umejiaku, M. Anyaegbe, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria,' (2010) *Nnamdi Azikwe University Journal* 18.
[23] Suit No: CA/245/05 available at http://www.cenbank.gov.ng/419/cases.asap. (accessed on 18 Sept. 2019 at 2pm).
[24] M. Chawki, 'Nigeria Tackles Advance Fee Fraud,' (2009) 1*Journal of Information Law and Technology* 10.

systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer based activities', and to impose liability for global crimes committed over the Internet and the Bill requires all service providers to record all traffic and subscriber information, and to release this information to any law enforcement agency on the production of a warrant.[25] Such information may only be used for legitimate purposes as determined by a court of competent jurisdiction, or other lawful authority and the Bill does not provide independent monitoring of the law enforcement agencies carrying out the provisions, nor does the Bill define 'law enforcement agency' or 'lawful authority.[26] Finally the Bill does not distinguish between serious offences and emergencies or minor misdemeanors as a result it may conflict with Article 37 of Nigeria's Constitution, which guarantees the privacy of citizens including their homes and telephone conversations, absent a threat on national security, public health, morality, or the safety[27]

Advanced Fee Fraud and Other Related Offence Act 2006

Another relevant legislative measure in the fight against fraud on the internet is the Advanced Fee Fraud and other Fraud Related Offences Act 2006. This is a replacement of an Act of the same title passed in 1995.[28] The act prescribes, among others, ways to combat cybercrime and other related online frauds and the Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretence, use of premises, fraudulent invitation, laundering of fund obtained through unlawful activity, conspiracy, aiding, etc. Section 2 of the Act makes it an offence to commit fraud by false representation.[29] Subsection (2) (a) and (2) (b) makes it clear that the representation must be made with intent to defraud while Section 3 of the Act makes it an offence if a person who is being the occupier or is concerned in the management of any premises, causes or knowingly permits the premises to be used for any purpose constitutes an offence under this Act.[30] This section provides that the sentence for this offence is imprisonment for a term of not more than 15 years and not less than five years without the option of a fine.[31] Section 4 refers to the case where a person who by false pretence, and with the intent to defraud any other person, invites or otherwise induces that person or any other person to visit Nigeria for any purpose connected with the commission of an offence under this Act, and the sentence for this offence is imprisonment for a term not more than 20 years and not less than seven years without the option of a fine.[32]

According to Section 7[33], a person who conducts or attempts to conduct a financial transaction which involves 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, the location, the source, the ownership or the control of the proceeds of a specified unlawful activity is liable on conviction to a fine of one million naira and in the case of a director, secretary or other officer of the 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.[34] In the earlier law being the 1995 Act, the onus is on the government to carry out surveillance on such crimes and alleged criminals but the new law that is the 2006 Act vest this responsibilities on industry players, including cybercafé operators, among others.[35] While the Economic and Financial Crimes Commission (EFCC) becomes the sub-sector regulator, the Act prescribes that henceforth, any user of Internet services shall no longer be accepted as anonymous.[36] Through what has been prescribed as due care measure, cybercafé operators will henceforth monitor the use of their systems and keep a record of transactions of users and these details include, but are not

[25] ibid.
[26] ibid.
[27] ibid.
[28] M. Chawki, 'Nigeria Tackles Advance Fee Fraud,' (2009) 1 *Journal of Information Law and Technology*. p. 10.
[29] ibid.
[30] ibid.
[31] ibid.
[32] ibid.
[33] Advanced Fee Fraud and Other Related Offences Act 2006.
[34] ibid.
[35] M. Chawki, 'Nigeria Tackles Advance Fee Fraud,' (2009) 1 *Journal of Information Law and Technology*. p. 10
[36] ibid.

limited to, photographs of users, their home address, telephone, email address, etc.[37] So far, over 20 cybercafés have been raided by the EFCC as of August 7, 2007 and the operators appear set to comply with the law by notifying users of the relevant portion of the law, corporate user policy, firewall recommendation, protection procedure, indemnity and right of disclosure, and so forth.[38] From the mentioned provisions, it can be seen that though the Advanced Fee Fraud and Other Related Offences Act effectively deals with related online fraud, the Act still does not go a long way in dealing with cybercrimes.

Money Laundry (Prohibition) Act 2011

Another related law regulating the internet scam is the Money Laundering (Prohibiting) Act 2011. 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 while Section 17 and Section 18 of the Act also implicates any person corporate or individual who aids or abet illicit disguise of criminal proceeds.[39] However Section 10 of the Act makes activities difficult for money launderers by mandating financial institutions to make compulsory disclosure to National Drugs Law Enforcement Agency 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.[40] This enables authorities to monitor and detect suspicious cash transactions on internet and these sections can be used against criminals who use the internet as a means of unlawfully transferring large amount of money from one account to another.[41] However the Act does not effectively deal with the cybercrime activities on the internet.

Penal Code (Kano State) 1960

This section gives a critical overview of Nigeria which adopted penal laws in prosecuting cybercriminals and if such laws are not adequate to target "high profile" cybercrimes such as virus dissemination, hacking, fraud and theft, then Nigeria have an imperative to review their penal laws to ensure that their citizens are well protected from cybercriminals, as internal prosecutors have been known to fail for lack of applicable law.[42] In the case of *United States v Baker*[43] the U.S Federal courts of appeals upheld dismissal of charges against a defendant who posted descriptions of his raping, torturing and killing of women online because provisions of federal criminal statute did not encompass his actions.[44] If a country reviews its penal laws and it indicates a lacuna which does not effectively deal with cyber-crime, steps should immediately be taken to amend the deficiencies by adopting new cybercrime laws and amending existing laws, and it is relevant to mention at this point that countries ignoring this grey area of the law will definitely be less able to compete in the new economy, reason being that cybercrime increasingly breaches national borders and nations perceived as havens run the risk of having their electronic messages blocked by the network.[45] The penal sanctions against trespass or breaking and entry cannot hold against an act of hacking into a computer network and unlawfully acquiring data.[46] From sophisticated airline reservations systems, military early warning mechanisms to the Automated Teller Machines (ATM) and the digital supermarket till, the Information Technology (IT) revolution has brought about a vast array of aides and conveniences that have always influenced modern communication, travel, security and commerce, however the massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever present risk of abuse,

[37]ibid.
[38] ibid.
[39] Money Laundering (Prohibition) Act 2011.
[40] Money Laundering Act 2011 9 (as amended).
[41] ibid.
[42] A, Laura, 'Cyber Crime and National Security: The Role of the Penal Code and Procedural Law' (2011) 2 Law and Security in Nigeria 206.
[43]1997 Fed. App. 0036P (Sixth Circuit Court of Appeals 1997) see: www.laws.lp.findlaw.com. (Accessed on 12 Oct. 2020).
[44] ibid.
[45] ibid (n 42).
[46] ibid.

insidious manipulation and sabotage of computer and computer networks.[47] This distinct, unitary phenomenon is a new class of anti-social activity that cannot be dealt with through the application of extant laws and most countries lack appropriate legislation to deal with internet/computer related crimes.[48] The critical question is how do one apply the traditional provisions of the Penal Code to offences related to cybercrime, for instance the offence of theft or stealing requires that tangible property to be taken away with the intention of permanently depriving the victim of it.[49] Applying traditional Penal Code concepts to acts involving intangible information can only mean that amendments to our Penal Statutes are unavoidable hence in order to strengthen this point a look at Section 484 of the Criminal Code, Section 321 and 342 of the Penal Code and Section 348 of the Shari'ah Penal Code Law of Zamfara State, which deal with personating and criminal trespass reflects the shortcomings of our criminal sanctions to effectively deal with cyber-crime.[50]

Criminal Code Act 1990

The Criminal Code Act of 1990 criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber-crime is not mentioned in the Act, it is a type of stealing punishable under the criminal code.[51] Betting, theft and false pretences performed through the aid of computer networks are also the type of crimes punishable under this Code however Sections 239(2) (a) and 240(a) of the Code prohibit betting and public lotteries respectively. Therefore Section 239(2)(a) provides that any house, room or place which is 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.[52] However these sections can be used by law enforcement agencies to regulate 'online betting' or prosecute such persons as would contravene this Section.

However public lottery is defined under Section 240 of the Act to mean that which the public or any class of the public has, or may have access and every lottery shall, until contrary is proved be deemed to be a public lottery.[53] Lottery includes any game, method or device whereby money or money's worth is distributed or allotted in any manner depending upon or to be determined by chance or lot while Section 240a of the Act also provides that every person who writes, prints, publishes or causes to be written, printed or published, any lottery ticket or any announcement relating to public lottery shall be liable to a fine not exceeding six (6) months.[54] These sections also cover lotteries which are mostly done with the use of computers or on the internet in this modern world as being an offence and can be used to combat this cyber-crime. The most renowned provision of the Act is Chapter 38, which deals with obtaining property by false pretences and cheating. The specific provisions relating to cyber-crime is Section 419 of the Act, while Section 418 of the Act gave a definition of what constitutes an offence under the Act however Section 418 states 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, while Section 419 of the Act states that 'any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.'[55] However Section 383(1) of the Act states that a person who fraudulently takes anything capable of being stolen,

[47]ibid.
[48]ibid.
[49] ibid.
[50] ibid.
[51] O, Sam, 'Cybercrimes and Cyber Laws in Nigeria' (2016) 2 *International Journal of Engineering and Science* 22.
[52] Criminal Code Act 1990.
[53] ibid.
[54] ibid.
[55] O Sam, (n 51).

or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing.[56] These sections also covers false pretence and fraud which is done with the aid of computer on internet as being an offence, but has not effectively deal with cybercrime although the section can be used to combat these crimes.

Evidence Act 2011

The 2011 Evidence Act is an amendment of the 1945 Evidence Act which did not provide for the admissibility of electronically generated evidence but there is a provision in the 2011 Evidence Act for the admissibility of digital and electronic evidence, but electronically generated evidence was not admissible in Nigeria court before the enactment of the 2011 Act, and this has created a serious difficulty in the prosecution of cybercrimes in Nigeria.[57] In the case of *Esso West Africa Inc. v. T. Oyegbola*[58]**,** the court had a foresight when it stated that: 'the law cannot be and is not ignorant of the modern business methods and must not shut its eyes to the mysteries of computer. In modern times reproduction and inscriptions on ledgers or other documents by mechanical process are common place and Section 37 cannot therefore only apply to books of account'.[59] The Evidence Act is therefore a huge step towards a right direction in the prosecution of cybercrime activities in Nigerian courts and following the long-awaited call for review of evidence laws to become age compliant, the Nigeria court now admit digital evidence. The 2011 Act provides for the definition of a computer which was not included in the 1945 Evidence Act, however under the 2011 Act, a computer is defined 'as any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process'.[60] Section 84(1)-(5) of the Act provides for the admissibility of statements in documents produced by computers and the section has now made it possible for facts for which direct oral evidence can be given to be equally evidence by a computer-produced document containing such facts, subject however to condition precedents as to the document, the computer from which it was generated and the person who generated it or manages the relevant activities captured in the document, for instance cybercafé managers, secretaries, ATM card users or experts.[61] Section 84(2) of the Act provides for a condition for the admissibility of statement in documents produced by computers which is very comparable to the position in England on the admissibility of computer generated evidence, however this is to the fact that the Nigerian law today is more or less a mixture of the English law.[62] Thus, in *R v. Spiby*[63] the English Court of Appeal held that the trial judge had properly admitted evidence of computer printouts of a machine which had monitored hotel guests' phone calls, Taylor L J in this case confirmed that 'this was not a printout which depended in its content for anything that had passed through the human mind' and so was admissible as real or direct evidence.[64] The court also noted here that unless there was evidence to the contrary the court would assume that the electronic device generating the evidence was in working order at the material time.[65] Legal Practitioners can now make use of Section 84(5) of the Act to establish that information via mobile phones and other gadgets and devices are admissible and this has made it more convenient and expedient for our courts to admit computer generated evidence although the Act did not effectively deal with cybercrime.

Cybercrime (Prohibition, Prevention Etc) Act 2015

The general laws that are not specifically related to cybercrime but are being enforced to deal with cyber-crimes which have being discussed above, have to a large extent not being effective in curbing cybercrime. In a proposal to put in place a stronger legal framework to control cybercrime, a revision of the existing cybercrime legislation was put forward by the Government in September 2008.[66]

[56] ibid.
[57] ibid.
[58] (1969) NMLR 194 at pp 216-217.
[59] (1969) NMLR 194 at pp 216-217.
[60] Section 258 of the Evidence Act 2011.
[61] O, Elias, 'The Law in a Developing Society,' (1969) 3 University of Lagos Law Journal 5.
[62] ibid.
[63] (1990), 91 Criminal Appeal Review 186.
[64] ibid.
[65] (1990), 91 Criminal Appeal Review 186.
[66] A. Olubukola, 'Cyber Crime and Poverty in Nigeria,' (2017)13 *Canadian Social Science* p26.

However the bill titled "A Bill for an Act to provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters" passed second reading in November 2012 at the Senate.[67] 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.[68] The Act is known as the Cybercrimes (Prohibition, Prevention etc.) Act 2015 and it creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters particularly, the Act prompt 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.[69] The Cybercrimes Act 2015 is, thus, the first legislation in Nigeria that deals specifically with cybercrimes and cyber security. The Act, stipulates that, any crime or injury on critical national information infrastructure, sales of pre-registered Subscribers Identification Module (SIM) cards, unlawful access to computer systems, Cyber-Terrorism, among others, would be punishable under the new law. The Act prescribes stringent penalties for offenders and perpetrators of cybercrime.[70] The Cybercrimes Act is made up of 59 Sections, 8 Parts; and 2 Schedules, the 1stSchedule lists the Cybercrime Advisory Council; second Schedule lists businesses to be levied for the purpose of the Cyber-security Fund, which is provided under Section 44 (2) (a) and these businesses include; Global System Mobile (GSM) service providers and all telecom companies; internet service providers; banks and other financial institutions; insurance companies; and Nigeria Stock Exchange (NSE).[71] According to Section 6 of the Act, hackers, if found guilty of unlawfully accessing a computer system or network are liable to conviction to a term of not more than 5 years imprisonment or to a fine of not more than 5 hundred thousand Naira nor to both. While Section 22 of the Act provide for identity theft and impersonation, that any person found guilty would be liable to punishment of imprisonment to a term of 7 years or to a fine of not more than 5 hundred thousand Naira or to both, similarly the Act in Section 5 prescribes conviction to imprisonment for a term of not more than 10 years without an option of fine for any person found guilty of the offence against critical national information infrastructure.[72] However Section 24 of the Act provides for outlaws cyber stalking and cyber bullying and prescribed punishment of conviction of not more than 3 years imprisonment or to a fine of not more than 7 Hundred Thousand Naira or to both. While Section 25 provide for cyber-squatting and any person found guilty under this section would be liable for a conviction to a term of not more than 2 years imprisonment or to a fine of not more than five Hundred Thousand Naira or to both, and Section 23 of the Act provides for child pornography, it specifically create child pornography offences with punishment of imprisonment for a term of 10 years or a fine of not more than 20 million Naira or to both. It makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than ₦7 million or to both fine and imprisonment.[73]

Apart from the Cybercrimes Act, the Economic and Financial Crimes Commission (EFCC) has also been monitoring and raiding internet cafes, and in most cases, stopping night browsing at the cafes and according to the former Chairman of the commission, Ibrahim Lamorde, more than 288 persons have been convicted for various cases of cybercrime across the country; another 234 cases are still under prosecution in various courts nationwide while four fugitives have been extradited to the United States of America.[74]

3. Institutional Framework for Regulating Cybercrimes in Nigeria

There are certain bodies in Nigeria set up by the Nigerian government mainly involved in the setting-up of special bodies by the Nigerian government to deal with cybercrime. And they include the Economic and Financial Commission (EFCC) and the Nigerian Cybercrime Working Group.

[67] ibid.
[68] ibid.
[69] ibid.
[70] A. Olubukola, 'Cyber Crime and Poverty in Nigeria,' (2017)13 *Canadian Social Science* 26.
[71] ibid.
[72] Cyber Crimes (Prohibition, Prevention etc.) Act 2015.
[73] Cyber Crimes (Prohibition, Prevention e.t.c) Act 2015.
[74] A, Olubukola, 'Cyber Crime and Poverty in Nigeria,' (2017)13 *Canadian Social Science* 26.

Economic and Financial Crime Commission

The Economic Financial Crime Commission (EFCC) is a Nigerian law enforcement agency that investigates financial crimes such as advance fee fraud and money laundering.[75] The commission is empowered to investigate, prevent and prosecute offenders who engage in money laundering, embezzlement, bribery, looting and any form of corrupt practices, illegal arms deal, smuggling, human trafficking, and child labour, illegal oil bunkering, illegal mining, tax evasion, foreign exchange malpractices include counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes, and prohibited goods, the commission is also responsible for identifying, tracing, freezing, confiscating, or seizing proceeds derived from terrorist activities. For example, in 2005, the EFCC confiscated at least hundred million dollars from spammers and other defendants.[76] Punishment prescribed in the EFCC Establishment Act range from combination of payment of fine, forfeiture of assets and up to five years conviction for terrorist financing and terrorist activities attract life imprisonment.[77] It must be stated here that EFCC has excellent working relationship with major Law Enforcement Agencies all over the world and these include United Nation on Drugs and Crime (UNODC), Economic Community of West African States (ECOWAS), Council of Europe (COE) among other agencies.[78]

Nigerian Financial Intelligent Unit (NFIU)

This is an operative unit in the office of EFCC and was established under EFCC Act 2004 and Money Laundering (Prohibition) Act of 2004, as amended and the unit is a significant component of the EFCC.[79] It complements the EFCC's directorate of investigations but does not carry out its own investigation.[80] The unit's coordinating objective is receipt and analysis of financial disclosure of currency transaction report and suspicion transaction and all financial institutions and designated non-financial institutions are required by law to furnish the Nigeria Financial Intelligent Unit with details of their financial transactions.[81] The Nigeria Financial Intelligent Unit has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centers.[82]

Nigeria Cybercrime Working Group (NCWG)

The Nigerian Federal government in 2004 set up the Nigeria Cybercrime Working group (NCWG) to realize the objectives of National Cyber-security Initiative (NCI).[83] The objectives of the National Cybercrime Initiative include public enlightenment of the Nigerian populace on the nature and danger of cybercrime, criminalization through new legislation of all on-line vices, establishment of legal and technical framework to secure computer systems and networks, and protection of critical information infrastructure for the country.[84] The group was created to deliberate on and propose ways of tackling the malaise of internet fraud in Nigeria and this includes: educating Nigerians on cybercrime and cyber security; undertaking international awareness programs for the purpose of informing the World of Nigeria's strict Policy on Cybercrime and to draw global attention to the steps taken by the Government to rid the country of Internet fraud in particular and all forms of cybercrimes; providing legal and technical assistance to the National Assembly on cybercrime and cyber security in order to promote general understanding of the subject matters amongst the legislators; carrying out institutional consensus building and conflict resolutions amongst law enforcement, intelligence and security Agencies in Nigeria for the purpose of easing any jurisdictional or territorial conflicts or concerns of duties overlap; reviewing, in conjunction with the Office of the Attorney General of the Federation, all

[75] M, Chawki, 'Nigeria Tackles Advance Fee Fraud,' (2009)1 *Journal of Information Law and Technology* 11.
[76] ibid.
[77] ibid.
[78] ibid.
[79] ibid.
[80] ibid.
[81] ibid.
[82] ibid.
[83] ibid.
[84] M. Chawki, 'Nigeria Tackles Advance Fee Fraud,' (2009)1 *Journal of Information Law and Technology*. p. 11.

multilateral and bilateral treaties between Nigeria and the rest of the World on cross-border law enforcement known as Mutual Legal Assistance Treaties (MLAT), for the purpose of amending the operative legal framework to enable Nigeria secure from, as well as render, extra-jurisdictional assistance to its MLAT Partners in respect of cybercrime. [85]

4. Conclusion

However, from what has been discussed above that there is no designated regulatory agency specifically set up for control cybercrime in Nigeria. Although some of the regulatory agency that are used to help control the menace of cybercrime are discussed but they are not that effective when it comes to cybercrime because they are not designated for controlling cybercrime. However the majors Federal Government has put in place by establishing the Nigerian Cybercrime Working Group comprising representatives from government and the private sector to develop legislation on cybercrime in 2004, and also in 2007, established the Directorate for Cyber Security, which is an agency responsible for responding to security issues associated with growing usage of internet and other information and communication technologies (ICTs) in the country which are working under the directives of the Economic and Financial Crime Commission are not effective in controlling cybercrime. As cybercrime is increasing daily and becoming a threat to the society the Federal Government there is need to set a regulatory body independent of EFCC with the sole responsibility of controlling cybercrime in Nigeria.

[85] Ibid.