International Journal of Diplomatic, Legal & International Studies
Volume 10, Issue 6, PP 1-8, ISSN: 2360-9163, February, 2025
DOI: 4272-1453-54-1061-1
Double Blind Peer Reviewed International Research Journal
Journal Series: Global Academic Research Consortium (garc)
arcnjournals@gmail.com
https://arcnjournals.org

LEGAL AND INSTITUTIONAL FRAMEWORK FOR CYBER SECURITY IN NIGERIA: AN APPRAISAL

Shettima Mustapha, Shehu Usman Ali and Adama Asingar Yusuf
Department of Languages and Liberal studies, Ramat Polytechnic, Miduguri

Abstract: *Prior to the Cybercrime Act 2015, there were no specific legislation on cybercrime in Nigeria. The Cybercrime (Prohibition, prevention etc.) Act, 2015 now Cybercrime Act, 2024 (as amended) was enacted to provide a unified legal framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes in Nigeria. This paper had an appraisal of the legal and the institutional framework for cybersecurity in Nigeria as well as the responsibility they are saddled with in order to ensure and safeguarding the Nigerian cyberspace. It also put forward observations and recommendations on how to further strengthen the existing institutional and legal framework to further fortify the Nigerian cyberspace from the existing and emerging cyber threats*.

Keywords: Cybercrime, Cybersecurity, Legal, Framework, Financial Institution.

2) Introduction

The use of computers and internet resources becomes part and parcel of the daily life engagements of millions of Nigerians and institutions serving the Nigerian federation. This increasing use of computers and internet resources comes with a lot of benefits to the extent that its use and reliance for effectiveness becomes necessary and inevitable. This positive development also gives rise to the ever increasing cases of cybercrime in Nigeria affecting every facet of the nation's economic development. This necessitated the development of a legal and institutional framework to combat these illicit activities frontally. The proliferation of cybercrimes is now a global threat.

Internet fraud, hacking, identity theft and various forms of cybercrimes constitute a serious risk and a viable threat to businesses, individuals, institutions and national security. In order to combat these crimes, Nigerian government established legal framework for addressing cybercrime in Nigeria. The Cybercrimes (Prohibition, Prevention etc.) Act of 2024 (as

amended) serves as the primary legislation governing cybercrimes in Nigeria.

This Act created various cyber offences and provides the legal basis for law enforcement agencies to investigate and prosecute criminals.

3) LEGAL FRAMEWORK ON CYBERCRIME IN NIGERIA

For decades, cybercrime has been a very serious issue of concern that negatively affected Nigerian economy and the social wellbeing of Nigerians. Nigeria has had many disjointed interventions and mechanisms put in place to combat cybercrimes in Nigeria until 2015 when Nigeria's primary legislation as far as cybercrime is concerned was enacted.

Before the enactment of the Act in the year 2015, the Economic and Financial Crimes Commission (EFCC), the Independent Corrupt Practices Commission (ICPC), the State Security Service (SSS) and the Nigeria Police Force (NPF) all played important roles in combating the growing trend of cybercrimes in Nigeria[1].

a. **The Cybercrimes (Prohibition, Prevention and Punishment) Act 2024 (as amended)** was passed and went into effect on May 15, 2015 and was later amended in 2024. The Act provides for uniform and comprehensive legal, regulatory framework in Nigeria for the prohibition, detection, prosecution and punishment of cybercrime. The legislation also protects essential national information infrastructure, promotes cyber security and protects computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights[2].

   The 2024 amendments introduce some form of institutionalized response by establishing National Computer Emergency Response Team (ngCERT) and Security Operation Centers (SOCs) to respond to cyber-attacks. The two establishments are to work in synergy. The amended Act placed the responsibility of establishing and coordinating these centers on the office of the National Security Adviser (ONSA).

b. **Economic and Financial Crimes Commission (Establishment) Act 2002**[3]. This Act has 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 known as the EFCC. Section 5 of the Act charges the

[1] Olisa Agbakoba Legal: The Legislative Framework for Cybercrime in Nigeria: Current Status, Issues and Recommendattions. www.mondaq.com visited 15th November, 2024

[2] ibid

[3] Cap. E1, Laws of the Federation of Nigeria,2010.

Commission with the responsibility of enforcement and due administration of the Act, the investigation of all financial crimes including advanced fee fraud, money laundering, counterfeiting, illegal change transfers and also the prosecution of all offences connected with or related to economic and financial crimes in consultation with the Attorney General of the Federation. The criminal activities under these economic crimes would include the activities of "yahoo boys" whose activities are sabotage on the economy of the country[4].

c. **Advanced Fee Fraud and Other Fraud Related Offences Act 2006**[5]. The Act was enacted to prohibit and punish certain offences pertaining to advanced fee fraud and other fraud related offences and to repeal other Acts related therewith. Advanced fee fraud is a vexing threat and a major problem in Nigeria today[6]. The Act provides for ways to combat cybercrimes 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 activities, conspiracy, aiding among other crimes[7]. Section 2 of the Act 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 criminal identities while using the large drove of information on the internet to commit fraud[8].
d. **Money Laundering (Prohibition) Act 2010**[9] is another legislation regulating internet related frauds. It contains provisions to criminalize the acts of laundering the proceeds of illegal activities. It prohibits the concealing or hiding the sources of resources or properties which are proceeds of illegal acts under Nigerian law. Section 18 of the Act placed criminal responsibility on any individual or corporate body that engages in the offering of aids or provides their platforms for disguising proceeds of criminal activities.

[4] Ehimem R. and Bila A., Cybercrimes in Nigeria, Business intelligence Journal, (2010) 3(1), pp.93-98.
[5] Cap. A6, Laws of the Federation of Nigeria,2010.
[6] Chawki, M., Nigeria Tackles Advance Fee Fraud, Journal of Information, Law and Technology, (2009) 1, pp.1-20.
[7] Obidimma and Ishiguzo: Legal and Institutional Framework for Cybersecurity Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures, Journal of Information, Law and Technology, (2009) 1.

[88] Ibid.
[9] Cap. M18, Laws of the Federation of Nigeria, 2010.

The Act also made it an obligation on financial institutions to make disclosures to National Drug Law Enforcement Agency (NDLEA) in certain prescribed circumstances.

e. **Evidence Act 2011** the Nigerian Evidence Act repealed the defunct Evidence Act of 1945. Unlike the repealed Act, the Evidence Act 2011 allows for the admissibility of electronically generated data as evidence before any court of law or tribunal in Nigeria. Hitherto, electronically generated evidence was inadmissible in Nigerian courts resulting in creating obstacles in the effective prosecution of cybercrimes in Nigeria.
f. **Independent Corrupt Practices and other offences Commission (ICPC) Act 2000.** The ICPC Act seeks to prohibits and prescribe punishment for corrupt practices and other related offences. The nexus between cybercrime and the ICPC Act may not be elaborate as the ICPC Act provides for some few offences that are internet related or can only be committed through the use of the computer networking and the internet. While it does not address cybercrime but it contains some provisions that can be deployed in the fight against cybercrime.

INSTITUTIONAL FRAMEWORK FOR CYBERCRIME IN NIGERIA

1. **Office of the Attorney General of the Federation:** The Attorney General of the Federation is the Chief Law Officer of the Federation and represents the office of the Attorney General of the Federation as an institution created by the Constitution of the Federal Republic of Nigeria 1999 (as amended). The office of the Attorney General of the Federation is created by section 174 of the Constitution of the Federal republic of Nigeria and clothed with all the prosecutory powers and authorities of the federation. The Cybercrime Act 2015 also surrendered all the prosecutory authority of cybercriminals under the Act to the office of the Attorney General of the Federation. The office of Attorney General of the Federation ensures not just the prosecution of persons and entities accused of cybercrime but also ensures that all assets and proceeds of cybercrime convict are forfeited to the federal government effectively[10].
2. **The Economic and Financial Crimes Act (EFCC):** The Economic and Financial Crimes Commission Establishment Act contains elaborate provisions that empowers the commission with extensive investigative and prosecutorial powers with respect to financial and

[10] Section 48(2) and (3) of the Cybercrime Act 2015.

econ omic crimes generally and cybercrime in particular as most of the financial crimes are committed using the Nigeria's cyberspace. From its establishment to date, the Commission has effectively arrested, investigated and successfully prosecuted cyber related criminals. One case to demonstrate this giant stripes of the commission as far as cybercriminals in Nigeria are concerned is the case of Harrison Odiawa Vs. FRN[11] and Amadi Vs. FRN CA/L/389/2005.

The recent arrest of nearly 800 cybercrime suspects by the Economic and Financial Crimes Commission (EFCC) marks a significant milestone in Nigeria's fight against internet fraud. The Victoria Island operation led to the arrest of 792 suspects including 148 Chinese and 40 Filipino nationals, represents the largest single raid in the commission's history. The international dimension of the arrest reveals the evolving nature of cybercrime on Nigerian soil and highlights the complex web of cross-border criminal enterprises[12]. The seizures of computers, phones and vehicles in the Victoria Island raid provides valuable evidence that could lead to further revelations. However, the EFCC's historical record shows a concerning gap between arrests and convictions. Critics have questioned both the commission's expertise and its commitment to prosecuting cyber frauds and political corruption cases[13].

3. **NIGERIA FINANCIAL INTELLIGENCE UNIT**: The NFIU is the Nigerian arm of the global financial intelligence units (FIUs)[14]. It seeks to adhere international standards on combating money laundering, financing of terrorism and proliferation. It was established in 2005 by the EFCC and domiciled as an autonomous unit operating in African region. The EFCC Act of 2004 and the Money Laundering (Prohibition) Act 2011 (as amended) confer powers on the NFIU[15]. The unit was established based on the recommendation 29 of the Financial Action Task Force (FATF) standard and Article 14 of the United Nations Convention Against Corruption (UNAC)[16]. It formulates coordinated policies that aim to

[11] (2008) LPELR-CA
[12] www.blueprint.ng accessed on the 10th January,2025.
[13] Ibid.
[14] http://www.nifu.gov.ng//index.php/nifu accessed on the 25th December, 2024.
[15]Obidimma and Ishiguzo: Legal and Institutional Framework for Cybersecurity Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures, Journal of Information, Law and Technology, (2009) 1.
[16] Ibid.

combat money laundering, terrorists financing and serious financial crimes. In 2018, former President Muhammadu Buhari signed the Nigerian Financial Intelligence Unit Bill (NFIU) 2018 into law[17]. The signing of the new Act makes National Financial Intelligence Unit (NFIU) independent of the Economic and Financial Crimes Commission (EFCC). The Act creates NFIU as the central body in Nigeria responsible for requesting, receiving, analyzing and disseminating financial intelligence reports and other information to all law enforcement, security and intelligence agencies and other relevant authorities.

4. **NIGERIA CYBERCRIME WORKING GROUP**: The Nigeria Cybercrime Working Group (NCWG) is an establishment of the Federal Executive Council (FEC) on the recommendation of the then president of Nigeria on 31st March,2004. It is an inter-agency body comprising all key law enforcement, security, intelligence and ICT and ICT organisations. The group was created to seek ways of tackling the menace of 419 frauds in Nigeria[18].
5. **CYBERCRIME ADVISORY COUNCIL**: The Cybercrime Act established Cybercrime Advisory Council which consists of a representation of different ministries and agencies listed in the Act. The representatives as required from each ministry shall be an officer not below the Directorate cadre in the public service or its equivalent and the functions and powers of the council includes the following: advice on the measures to prevent and combat computer related offences, crimes, threats to national cyberspace and other cybersecurity related issues; establish a program to award grants to institution of higher education to establish cybersecurity research centers to support the development of new cybersecurity defenses, techniques and processes in the real world environment; and to promote graduate traineeships in cyber security and computer network security research and development[19].
6. **COMPUTER PROFESSIONALS REGULATION COUNCIL**: section 7(1)(a) of the Cybercrime Act, 2024 (as amended) empowers the Computer Professionals Registration Council to register all operators of cyber café as a business in addition to a

[17] http://www.dailytrust.ng accessed on 25th December,2024

[18] Obidimma and Ishiguzo: Legal and Institutional Framework for Cybersecurity Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures, Journal of Information, Law and Technology, (2009) 1.

[19] Cybercrime Act ss.42 and 43

business name registration with the Corporate Affairs Commission and in a way of checkmating the activities that goes on at cyber café, the operators are also mandated in addition to the above mandatory registration, to maintain a register of users through a sign in register and such register must be made available to law enforcement personnel whenever needed and to further keep the operators alive to their responsibility of ensuring that internet fraudsters do not use their cyber café as a base for their heinous activities, the law provides that in the event of such, owners shall be liable to a fine of N2,000,000.00 or imprisonment for a term of 3 years or both.

7. **NIGERIA POLICE FORCE (NPF)**: is the creation of the Nigerian Constitution and empowers it with powers to investigate and prosecute all forms of criminal activities within the Federal Republic of Nigeria irrespective of whether such criminal activity is in respect of laws of the federation, states or any local government area in Nigeria. The Nigeria Police Force has a specialized unit dedicated to countering cybercriminal activities in Nigeria. The Special Fraud Unit (SFU) which is charged with the responsibility of apprehending and carrying out forensic investigation at cybercriminal activities in Nigeria[20].
8. **FINANCIAL INSTITUTIONS**: financial institutions owe a duty of care towards their customers by ensuring that effective counter-fraud measures are put in place to safeguard the interest of their customers as well as the interest of their institutions. Any financial institution found not to have put in place measures that will prevent cybercriminal activities that will negatively impact on the interest of their clients would be held responsible for negligence[21].
9. **CONCLUSION**

   Cybercriminal activities has been an evolving criminal phenomena that requires legislators, regulators and law enforcement agencies to always remain proactive to effectively counter existing and emerging threats to ensure the safety of Nigeria's cyberspace. Regular review of legislation, increased investment in cybersecurity infrastructure, training and retraining of security personnel and cybersecurity experts remains

[20]Obidimma and Ishiguzo: Legal and Institutional Framework for Cybersecurity Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures, Journal of Comparative Law and Legal Philosophy (IJOCLLEP) 5(1) 2023.

[21] Section 19(3) of the Cybercrime Act, 2015.

necessary on the part of government to boost confidence and engender trust in the Nigerian cyberspace which is a prerequisite for security and overall national development.

10. Observations

In the course of this research, the following observations are noted thus:

a. There is no centralized and dedicated agency of the government in terms of providing coordinated response to cyber security threats and challenges.
b. As a result of the absence of centralized body in the fight against cybercrime in Nigeria, there is no proper synergy among key stakeholders involved in the fight against cybercrime

11. RECOMMENDATIONS

The following recommendations are made thus:

a. There is need for the legislature to further review the Cyber Security Act, 2024 (as amended) by providing stiffer penalties for those found guilty. The penalties are insufficient and effective to serve as deterrence particularly as the proceed of cybercrimes are mostly in hard currencies.
b. There is a case of insufficient technical proficiency considering increasing sophistication of cyber-attacks and rapidly evolving technology. Therefore, there is need for increased investment in technical skill training and retraining.
c. There is need for the establishment of a centralized institution solely charged with the responsibility of preventing, detecting, reporting and prosecuting cyber criminals in Nigeria.