CYBERCRIME AND THE EXERCISE OF CRIMINAL JURISDICTION IN NIGERIA: A DOCTRINAL ANALYSIS*

Abstract

The rapid expansion of information and communication technology has transformed patterns of criminal behaviour, giving rise to cybercrimes that operate beyond traditional territorial boundaries and pose significant challenges to conventional criminal jurisdiction. In Nigeria, the growing incidence of cyber-enabled offences has compelled the legal system to adapt existing jurisdictional principles to the realities of cyberspace. This article undertakes a doctrinal analysis of the exercise of criminal jurisdiction over cybercrimes under Nigerian domestic law. It examines the conceptual foundations of cybercrime, cyberspace, and cyber-jurisdiction, as well as the constitutional and statutory frameworks regulating cybercrime prosecution in Nigeria. Particular attention is paid to the exclusive and unified jurisdiction of the Federal High Court as established by the Constitution of the Federal Republic of Nigeria 1999 (as amended) and reinforced by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and allied legislation. The article further analyses the extraterritorial reach of Nigerian cybercrime laws, the role of extradition, and the significance of international cooperation in combating transnational cyber offences. It argues that while Nigeria has developed a relatively comprehensive legal framework for addressing jurisdictional challenges associated with cybercrime, practical constraints relating to enforcement capacity, institutional coordination, and cross-border cooperation remain. The article concludes that sustained legal reform, capacity building, and enhanced international collaboration are essential to ensuring the effective administration of criminal justice in the digital age.

Keywords: Cybercrime, Criminal Jurisdiction, Doctrinal Analysis, Nigeria

1. Introduction

The rapid advancement of information and communication technology has fundamentally transformed social, economic, and governmental interactions across the globe.[1] While these technological developments have enhanced efficiency, connectivity, and access to information, they have also given rise to new forms of criminality commonly referred to as cybercrimes.[2] Cybercrimes, by their very nature, transcend territorial boundaries, operate within the virtual domain of cyberspace, and often involve multiple jurisdictions simultaneously.[3] This borderless character of cyberspace presents profound legal and jurisdictional challenges to traditional criminal justice systems that are largely premised on territorial sovereignty.[4]

In Nigeria, the proliferation of internet-enabled devices, increased digital financial transactions, and the widespread use of online platforms have made cybercrime a pressing national concern with serious implications for individual security, economic stability, and national sovereignty.[5] Consequently, the Nigerian legal system has responded through constitutional provisions, statutory enactments, and institutional frameworks aimed at preventing, investigating, prosecuting, and punishing cyber-related

***By Muhammad Mansur ALIYU, LLB, BL, LLM, PhD,** Department of Islamic Law, Faculty of Law, Usmanu Danfodiyo University, Sokoto; Email: muhammad.maliyu@udusok.edu.ng /mansurdtm@gmail.com; Tel: 08066060227 /08029054820; and

***Kabiru Ibrahim ABDULKADIR, LLB, BL, LLM,** No. 1388 Unguwar Jakada, Kano, Kano State, Email. kabiruibrahim737@gmail.com; Tel: 08033774510/08035179197

[1] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger Publishers 2010) 3–5.

[2] David Wall, 'Cybercrime and the Internet' in Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime* (Willan Publishing 2010) 5–7.

[3] Michael L. Rustad and Thomas H. Koenig, *Cybercrime and Internet Fraud* (2nd edn, West Academic Publishing 2015) 21–23.

[4] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (UNODC 2013) 11–14.

[5] A. T. Shehu, 'Cybercrime and the Challenge of Jurisdiction in Nigeria' (2019) 6(1) *Ahmadu Bello University Law Journal* 87, 90–91.

offences.[6] Central to this response is the issue of jurisdiction—particularly which courts possess the legal competence to adjudicate cybercrime matters, the scope of Nigeria's extraterritorial jurisdiction, and the mechanisms for international cooperation and extradition of cybercriminals.[7]

This article undertakes a critical analysis of cybercrime jurisdiction under Nigerian domestic laws.[8] It examines the conceptual foundations of cybercrime and cyberspace, the legal meaning of jurisdiction in the context of virtual offences, and the constitutional and statutory frameworks governing cybercrime prosecution in Nigeria.[9] Special attention is given to the role of the Federal High Court, the Extradition Act, the Cybercrimes (Prohibition, Prevention, etc.) Act, the Administration of Criminal Justice Act, and relevant institutional bodies.[10] The article further interrogates the adequacy of existing legal regimes in addressing jurisdictional conflicts arising from the transnational nature of cybercrime and evaluates Nigeria's capacity for effective enforcement within and beyond its territorial boundaries.[11]

2. Nature of Cybercrimes

Cybercrimes are crimes committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operation with malevolent programs committed with the realm of cyberspace or as offences committed through the medium of computer(s) and internet either with on inter connected network or otherwise, cybercrime is an offence committed by means of computer either as a tool or as a target of committing the offence(s).[12] Crimes committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or financial or other property loss to the victim directly or indirectly, using modern telecommunication networks such as internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth, SMS, MMS). Cybercrimes may threaten person or a nation's security and financial health. Therefore, cybercrimes are the wide range of malicious activities including the illegal interception of data, system interferences that compromise network indignity and availability,[13] Cybercrime is a kind of crime that happens in cyberspace, that is happens in the world of computer and the internet. Cybercrime has become a global phenomenon; this kind of crime has the serious potential for severe impact on our lives society and economy because our society is becoming an information society where communication takes place in cyberspace while there are several textbooks talking about cybercrime but only few literatures focus on the relevant laws to combat this seemingly uncontrollable phenomenon. In other words, most materials talk about cybercrime.[14]

3. Cyberspace

Cyberspace as a computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocol to facilitate data transmission and usage exchange. Cyberspace is also defined as a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange,

---

[6] Federal Republic of Nigeria 1999 (as amended); Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

[7] Extradition Act, Cap E25, Laws of the Federation of Nigeria 2004; Council of Europe, *Convention on Cybercrime (Budapest Convention)* (2001) arts 22–25.

[8] Muhammad Mansur Aliyu Esq. and Safiyya Ummu Mohammed 'Corrupt Practices in the Media, Traditional and Religious Institutions: A Legal Perspective', Law and Social Justice Review Vol. 3 (1) (LASJURE) 87 (2022) ISSN: 2564-7290, PP.87-94, available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/lwadsljerw3&div=16&id=&page=;Yemi Akinseye-George, *Legal System, Corruption and Governance in Nigeria* (New Century Law Publishers 2011) 214

[9] Oludayo Amokaye, *Criminal Procedure in Nigeria* (2nd edn, Princeton Publishing 2016) 312–314.

[10] Federal High Court Act, Cap F12, Laws of the Federation of Nigeria 2004; Administration of Criminal Justice Act 2015; Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

[11] UNODC (n 4) 215–218.

[12] A. M. Solomon, *Cyberlaw and the Enforcement of Legal Rights in Nigeria*, 3rd ed (Lagos: LexisNexis, 2019) at 5;

[13] Aliyu N.A., Cybercrime (s): New Threat to Electoral Democracy & Sovereignty of States, Department of Public Law, Bayero University, Kano.

[14] C. B. Nnama, 'The Jurisdictional Challenges of Prosecuting Cybercrime in a Digital Economy' (2022) 45:2 *Journal of Law and Technology* 120 at 120-121.

share, extract, use, eliminate information and disrupt physical resources.[15] This is a computer jargon used to represent hypothetical environment in which communication over the computer networks takes place.[16]

The advent of computers and the internet has opened a vast array of possibilities for the young and the old in the international community to have access to the world from their homes, offices, cyber cafes and so on. In recent times, internet or web-enabled phones and other devices like iPods, have made internet access easier and faster, not so long ago, computers were large, cumbersome devices utilized primarily by government, research and financial institutions. Nowadays, the technology ubiquitous and increasingly case to use, ensuring its availability to both offenders and victims.[17] The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way people perceived the world and changes the way we socialize and do business.[18]

Cyberspace means the environment where communication takes place using computer.[19] In other words, it is a world created by internet. Cyberspace can also be defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the internet, telecommunications networks, computer systems and embedded processors and controllers.[20] Cyberspace is a composition of various computer networks, Switches, routers, servers, etc. it is a cluster of various infrastructures such as transportation, banking, finance telecommunication, energy and public health.[21] According to Encarta, the term was coined by American writer, William Gibson and first used in his 1984 science fiction novel *Neuromancer*, in described cyberspace as a place of 'unthinkable complexity'.[22] Internet is said to exist in the cyberspace, hence all activities done through internet are said to be in the cyberspace. Cyberspace simply means virtual or notional domain where connected computers share electronic information.[23]

4. Cyber Jurisdiction

Jurisdiction is a territorial area of authority to hear and adjudicate on certain matters/cases, the internet, however has no territorial limitation as it crosses across every boundary of every nation. It is therefore a virtual world of interconnected computer networks, territorial jurisdiction on the cyberspace becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.[24]

---

[15]Ms. Heena Keswani 'Cybercrime: A Critical Study', (BBALLB, Final Year, University of Petroleum and Energy Studies, Dehradum, 2017) 132

[16]Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001).

[17] Muhammad Mansur Aliyu Esq., 'An Appraisal of the Legal Framework for the Protection of Children against Cyber Exploitation and Abuse', *A Compendium of Selected Articles on the Cybercrime Law and Digital Evidence with Related Legal Instruments,* A Book Published in Honour of Honourable Justice Audu Aboki JSC (Retired), 2022, pg.73-100; Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010), 9.

[18] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999), 64.

[19] OECD, *Understanding the Digital Divide* (OECD Publications 2001).

[20]David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).

[21] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Tallinn Manual on the International Law Applicable to Cyber Operations* (Cambridge University Press 2013), 91.

[22] Heena Keswani, 'Cybercrime: A Critical Study', (BBALLB), Final Year, University of Petroleum and Energy Studies, Dehradum, 2017) 133

[23] U.S. Department of Defense, *Joint Publication 3-12: Cyberspace Operations* (2018), 65; Muhammad Mansur Aliyu Esq., and Maryam Abdallah Wali, 'Institutional Framework of Fight Against Corruption Nigeria', Journal of Community & International Law (JCIL) Vol 2:1 2023, pp. 105 – 142, available at: https://journal.cfcomlaw.com/wp-content/uploads/2024/09/Aliyu-and-Wali-Institutional-Framework-2.pdfAliyu-and-Wali-Institutional-Framework-2.pdf

[24] Hema V. Menon, 'Cybercrime in the Indian Scenario and Indian Information Technology Act, 2008.' (Aayushi *International Disciplinary Research Journal,* 2016): 19

Jurisdiction connotes power of a court or tribunal to legally hear and determine/ adjudicate over a matter before her. Cyber jurisdiction means competence of a court of law or tribunal to hear and determine/adjudicate over a matter brought before her in relation to any business or transactions on the cyberspace. Jurisdiction is a matter of law; therefore, the law that established the courts or tribunals confers jurisdiction on the courts, tribunals and not otherwise. The parties before any court or tribunal cannot on their own, without any express provision of law confer jurisdiction on the courts or tribunals.

Jurisdiction' in legal parlance means the power of a court to hear or determine a case brought before it. Cyber-jurisdiction suggests the power to hear, determine and regulate activities in the cyberspace. To determine whether or not it can adjudicate over a subject matter, the court will consider the parties (personal jurisdiction), the place where the cause of arose (territorial jurisdiction), the cause of action itself (subject matter jurisdiction) and when the cause of action arose.[25]

5. Federal High Court Jurisdiction on Cyber Crimes

Nigeria is a constitutional democracy state, based on three tiers of government made up of the federal, state and local governments. The Constitution of the Federal Republic of Nigeria 1999 as amended, is foundation to the existence of all other laws in the Nigerian legal system. The Constitution expressly stipulates thus: 'This constitution is supreme and its provisions shall have binding force on the authorities and persons throughout the Federal Republic of Nigeria.'[26] The Constitution is therefore the tool by which the validity and legality of all existing laws, in the country, are determined, it is in that sense that the Constitution stipulates that if any other law is inconsistent with its provision is void, thus: 'If any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall, to the extent of the inconsistency, be void.[27]

By virtue of the provisions of the Constitution, the power to make laws and procedures regarding extradition of cybercrime suspects is vested exclusively in the Federal Government of Nigeria. Thus, the state and local governments are devoid of powers to legislate on matters connected to extradition of cybercrime suspects as this is within the exclusive powers of the federal government/National Assembly. Similarly, the Constitution confers adjudicatory powers over extradition matters on the Federal High Court to the exclusion of any other court of first instance.[28]

The jurisdiction of the Federal High Court over cybercrimes is rooted in both the Constitution and specific enactments by the National Assembly. As established in the landmark case of *CBN v. Njemanze & Ors*,[29] the Federal High Court possesses limited jurisdiction, meaning it only exercises powers expressly conferred upon it by the Constitution or through Acts of the National Assembly under Section 230(2) of the 1999 Constitution. This principle was further elucidated in *Peter v. C.O.P* [30] where the court held that the subject matter of a suit is the ultimate determining factor for jurisdiction. Under Section 251(1)(s) of the Constitution, the Federal High Court is empowered to exercise such other jurisdiction, civil or criminal, as may be conferred upon it by an Act of the National Assembly.

Specific Jurisdictional Provisions under the Cybercrimes Act

The primary statute governing this domain is the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015. Section 50 of the Act explicitly grants the Federal High Court the jurisdiction to try offences created under the Act. Notably, Section 50(1) provides that the court, located in any part of the Federation, shall have jurisdiction regardless of where the offence was committed, provided it meets certain criteria: (a) the offence was committed in the country; (b) on a ship or aircraft registered here; (c) by a citizen or

[25] Safiyya Ummu Muhamad and Muhammad Mansur Aliyu 'An Appraisal of the Legal Framework of Protection of Children's Rights in Nigeria', *African Journal of Law and Human Rights (AJLHR),* Vol. 6 (1) 2022, pp. 190-197, ISSN: 2630-709X. available at: (https://journals.ezenwaohaetorc.org/index.php/AJLHR/issue/view/148

[26] Section 1(1) of the Constitution of the Federal Republic of Nigeria 1999

[27] Section 1(3) Ibid.

[28] Section 251(1) (i) Ibid

[29] ((2025) LPELR-80696(SC)

[30] (2022) LPELR-56946(CA).

resident whose conduct would also be an offence in the country where it was committed; or (d) outside the country where the victim is a citizen or resident. This is complemented by Section 2 of the Act, which mandates that the provisions of the Act apply throughout the Federation.

Territorial Jurisdiction and the Concept of a Unified Court

A critical aspect of the Federal High Court's authority is its unified nature. In *Nwogu v. FRN*,[31] the court clarified that the Federal High Court is one single court with jurisdiction across the entire Federation. While the Chief Judge may create judicial divisions for administrative convenience under Section 19 of the Federal High Court Act, these divisions do not fragment the court's inherent territorial reach. This is particularly relevant for cybercrimes, which are often borderless. The case of *Ishola v. FRN*[32] reinforced this, stating that any division of the Federal High Court has the competence to try offences under the Cybercrime Act regardless of the specific location of the crime within the country.

Prosecutorial Authority and Regulatory Oversight

The enforcement of cybercrime laws involves specific procedural requirements. Section 47 of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 empowers relevant law enforcement agencies to prosecute offences, subject to the overarching powers of the Attorney General. However, for specific offences under Sections 19 and 21 of the Act, the approval of the Attorney General must be obtained prior to prosecution. Furthermore, Section 57 of the Act allows the Attorney General to make regulations for the efficient implementation of the Act, including the custody of electronic recordings and compliance with international conventions. This regulatory framework is supported by the Nigerian Judiciary Information Technology Policy Document, which emphasizes that the use of IT in the judiciary is no longer discretionary but a necessity for speedy justice.

Procedural Framework and Related Statutes

Beyond the Cybercrimes Act, other statutes reinforce the Federal High Court's role in the digital space. For instance, Section 31 of the Telecommunications and Postal Offences Act 1995 grants the court exclusive jurisdiction over telecommunications-related offences. Similarly, Section 103 of the Copyright Act 2022 vests exclusive jurisdiction in the Federal High Court for civil and criminal actions arising from digital intellectual property infractions. Procedurally, the Federal High Court (Civil Procedure) Rules 2019, specifically Order 58, empowers the Chief Judge to establish Communications and Service Centres for electronic filing. For criminal matters, the Federal High Court (Corruption and Other Related Offences) Sentencing Guidelines and Practice Direction ensures standardized sentencing for related financial and cyber-enabled crimes.

6. Federal High Court Jurisdiction on Cyber Crimes where Extradition is Involved

The Extradition Act, 1966, applicable to Nigeria is to provide for a comprehensive legal regime with respect to extradition of fugitive offenders including cybercrime suspects.[33] Extradition Act as the primary statute regulating extradition in Nigeria, it recognizes two separate categories of States. States in the first category are those that have an extradition agreement with Nigeria and in respect of which an agreement order has been made[34] and the second category consists of Commonwealth States.[35]This categorization is significant because while it is necessary to enter into separate and individual bilateral extradition treaties with States in the first category,[36] there is no such requirement for the second category of Commonwealth States.[37] Section 251(1) (i) of the Constitution grants the Federal High Court exclusive jurisdiction to entertain and determine all extradition related matters. The President (President Goodluck Jonathan) of Nigeria on 23 May 2014 issued an Executive Order to amend the Extradition Act. The Extradition Act (Modification) Order 2014 expressly modified the Extradition Act

[31] (2024) LPELR-73202(CA).
[32] (2021) LPELR-52838(CA).
[33] Preamble, Extradition Act 1966
[34] Section 1of Extradition Act, 1966.
[35] Section 2 Ibid.
[36] Section 1 of Extradition Act, 1966.
[37] Section 254 of the Constitution of the Federal Republic of Nigeria 1999.

(Modification) Order 2014 was promulgated pursuant to Section 315 of the Constitution which allows the President of Nigeria to modify any existing law so as to bring it into conformity with the Constitution.

The Federal High Court (Extradition Proceedings) Rules, 2015, the Rules empowers the Chief Judge of the Federal High Court to make procedural rules relating to matters over which the Federal High Court has jurisdiction. Although the Extradition Act has certain procedural provisions, they are inadequate to cover many areas of proceedings. The Federal High Court (Extradition Proceedings) Rules were made to ensure clarity in extradition proceedings and to promote efficient and expeditious hearing of extradition applications. Details of steps for extradition proceedings of which are not provided for by the Extradition Act are provided in the Federal High Court (Extradition Proceedings) Rules. It is however instructive that in terms of hierarchy of application, the Federal High Court (Extradition Proceedings) Rules is subordinate to the Extradition Act, and in the event of any conflict between the two, the Extradition Act will prevail.

The Evidence Act applies to all criminal proceedings with the exception of afield general court martial.[38] Extradition proceedings are not listed among the proceedings which are excluded from the application of the Evidence Act. The Evidence Act is therefore applicable to extradition proceedings before the Federal High Court, among other matters, the Evidence Act governs the admissibility and weight of evidence, the burden of proof in cybercrime as well as the competence and compellability of witnesses, relevance and admissibility of any piece of evidence. However, in proving the existence of foreign law, the Evidence Act is read in conjunction with the Extradition Act. By this exercise, the relevant foreign law is deemed to exist if mentioned in the warrant issued by the foreign court.[39] With regards to evidence in Nigeria needed for use in other countries.

The Federal High Court Act, 1973, which regulates the exercise of powers and general administration of the Federal High Court. Cybercrimes Act confers jurisdiction to try cybercrime on the Federal High Court, while the cybercrime suspect has to be extradited to Nigeria face his trial, the Federal High Court Act also confers exclusive jurisdiction over extradition on the Federal High courts in the country.[40] This is consistent with the provisions of the Constitution.[41] The Federal High Court Act has several provisions which are generally applicable to the Federal High Court and by this reason relevant to Federal High Court proceedings including extradition proceedings.

The Act empowers the Judge in extradition proceedings to compel any person present in Court to give evidence or produce any document in his possession or in to his power.[42]The person so ordered to testify or produce a document does not have to be a party to the extradition proceedings, where the person who is ordered to testify or produce documents refuses to comply, he/she may be punished by the Court.[43]

Section 51 of Cybercrimes Act provides that all offences under the Act are extraditable under the Extradition Act, therefore cybercrime is extraditable in light of the provision of the Act. The Act[44] also provides for mutual assistance and information sharing in respect of the offences under the Act and empowers the Attorney General of the Federation to request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences under the Act.[45]The also empowers the Attorney General of the Federation to forward to a competent authority of a foreign state

[38] Section 256 (1) (b) of Evidence Act, 2011
[39] Section 6(1) of Extradition Act, 1966
[40] Section 7(1)(i) of Federal High Court Act.
[41] Section 251 of the Constitution of the Federal Republic of Nigeria.
[42] Section 52 Ibid.
[43] Ibid.
[44] Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[45] Section 52(1) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015

any information obtained in the cause of investigation, if such information will assist in the investigation of cybercrime or any other offence under the Act without even prior request for the foreign state.[46]

The Administration of Criminal Justice Act (ACJA) 2015, regulates criminal procedure in federal courts including the Federal High Court which is by law has exclusive jurisdiction to try cybercrime offenders in Nigeria. Also, in relation to extradition, it also has exclusive jurisdiction, the ACJA is most relevant to procedural steps that relate to pre-proceedings and post-proceedings steps which are not provided for in either the Extradition Act or the Federal High Court (Extradition Proceedings) Rules. For example, there are protective provisions of the ACJA that are relevant to all persons who are denied their liberty on account of criminal accusations, proceedings or sanctions. One of such provisions relates to persons in detention pending extradition who will be included in the monitoring activities of the Administration of Justice Monitoring Committee.[47]

7. Institutional Regulatory Framework for the Prevention of Cybercrime in Nigeria

Under Nigerian legal regime of cybercrime powers to prevent cybercrime are vested on certain institutions as provided by Cybercrime Act.[48]

The institutions that prevent cybercrime according to the law are:

1. The Office of the National Security Adviser[49]
2. The Attorney General of the Federation[50]
3. Law enforcement, security and intelligence agencies[51] which comprise the following:
    i. State Security Service (SSS),
    ii. National Intelligence Agency
    iii. Defence Intelligence Agency
    iv. Nigerian Police Force
    v. National Drug Law Enforcement Agency
    vi. Nigerian Correctional Service
    vii. Nigerian Customs Service
    viii. Nigerian Immigration Service
    ix. Nigeria Security and Civil Defence Corps
    x. Economic and Financial Crimes Commission
    xi. Independent Corrupt Practices and other Related Offences Commission
    xii. National Agency for the Prohibition of Traffic in Person
    xiii. Defence Headquarters[52]
    xiv. judiciary[53]

8. Prosecution of Cybercrime in Nigeria

The law enforcement agency before the enactment of Cybercrimes Act, might manage to locate and arrest the cybercrime suspects, but to apprehend them might not be possible due to the lack of jurisdiction over them since jurisdictional issue is an issue of law, so therefore jurisdiction serves as an impediment to cybercrime prosecution. The power to prosecute cybercrime in Nigeria is vested on the relevant law enforcement agencies but subject to the powers of the Attorney General of the Federation.[54] The Office of the National Security Adviser serves a coordinating body for the prosecution of cybercrime in Nigeria.[55] All law enforcement, security and intelligence agencies in collaboration with the Office of the National Security Adviser, shall by law, develop requisite institutional capacity for

[46] Section 52(2) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[47]Section 469 and 470 of Administration of Criminal Justice Act (ACJA), 2015
[48] Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[49] Section 41(1) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[50] Section 41(2) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[51] Section 41(3) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[52] Section 41(3) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[53] Sections 45, 48 and 50 of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[54] Sections 47 and 41(2)(c) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[55] Section 41(1) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015

effective implementation of the provisions of Cybercrimes Act in prohibiting, preventing, detecting investigating and prosecuting cybercrime in Nigeria.[56] The only court to prosecute cybercrime in Nigeria is the Federal High Court located in any part of Nigeria regardless of where the offence of cybercrime is committed in so far as the offence is committed:

a) in Nigeria
b) in a ship or aircraft registered in Nigeria
c) by a citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence is committed
d) outside Nigeria, where-
    i. the victim of the offence is a citizen or resident of Nigeria; or
    ii. the alleged offender is in Nigeria and not extradited to any other country for prosecution.[57]

9. Conclusion

Cybercrime poses one of the most complex challenges to modern criminal justice systems, largely due to its borderless nature and the virtual environment within which it is committed. This article has demonstrated that while cyberspace operates beyond traditional territorial boundaries, criminal jurisdiction under Nigerian law remains firmly anchored in constitutional supremacy, statutory authority, and judicial interpretation. The Nigerian legal framework has made deliberate efforts to adapt conventional jurisdictional principles to the realities of cyber-enabled offences through constitutional provisions, legislative enactments, and institutional mechanisms. The analysis reveals that the Federal High Court occupies a central and exclusive position in the adjudication of cybercrime matters in Nigeria. This jurisdiction is constitutionally grounded and reinforced by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Extradition Act, and other allied statutes. The unified nature of the Federal High Court, coupled with the expansive jurisdictional reach conferred by the Cybercrimes Act, represents a pragmatic legal response to the transnational and non-territorial character of cybercrime. By permitting prosecution regardless of the physical location of the offence, victim, or offender—subject to statutory conditions—Nigerian law acknowledges the realities of digital criminality and seeks to prevent jurisdictional loopholes that could otherwise enable impunity. Furthermore, the article underscores the importance of extradition and international cooperation in addressing cybercrime. The designation of cybercrime as an extraditable offence, the exclusive jurisdiction of the Federal High Court over extradition proceedings, and the coordinating role of the Attorney General of the Federation collectively strengthen Nigeria's capacity to pursue cybercrime offenders beyond its borders. The applicability of the Evidence Act and the Administration of Criminal Justice Act to cybercrime and extradition proceedings further enhances procedural fairness, evidentiary certainty, and the protection of fundamental rights.

Notwithstanding these legal and institutional advances, significant challenges remain. Issues relating to enforcement capacity, technological expertise, inter-agency coordination, and delays in international mutual legal assistance continue to limit the effectiveness of cybercrime prosecution. The dynamic evolution of cyber threats also demands continuous legislative review, judicial innovation, and sustained investment in digital infrastructure and capacity building. In conclusion, Nigeria has established a robust domestic legal framework for the exercise of criminal jurisdiction over cybercrime, with the Federal High Court serving as the cornerstone of enforcement and adjudication. However, the effectiveness of this framework ultimately depends on its practical implementation, sustained institutional collaboration, and Nigeria's commitment to international cooperation. As cybercrime continues to evolve in scale and sophistication, the Nigerian legal system must remain adaptive, proactive, and responsive to ensure that the administration of criminal justice keeps pace with the realities of cyberspace.

[56] Section 41(3) of Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[57] Section 50 of Cybercrimes (Prohibition, Prevention, Etc) Act 2015