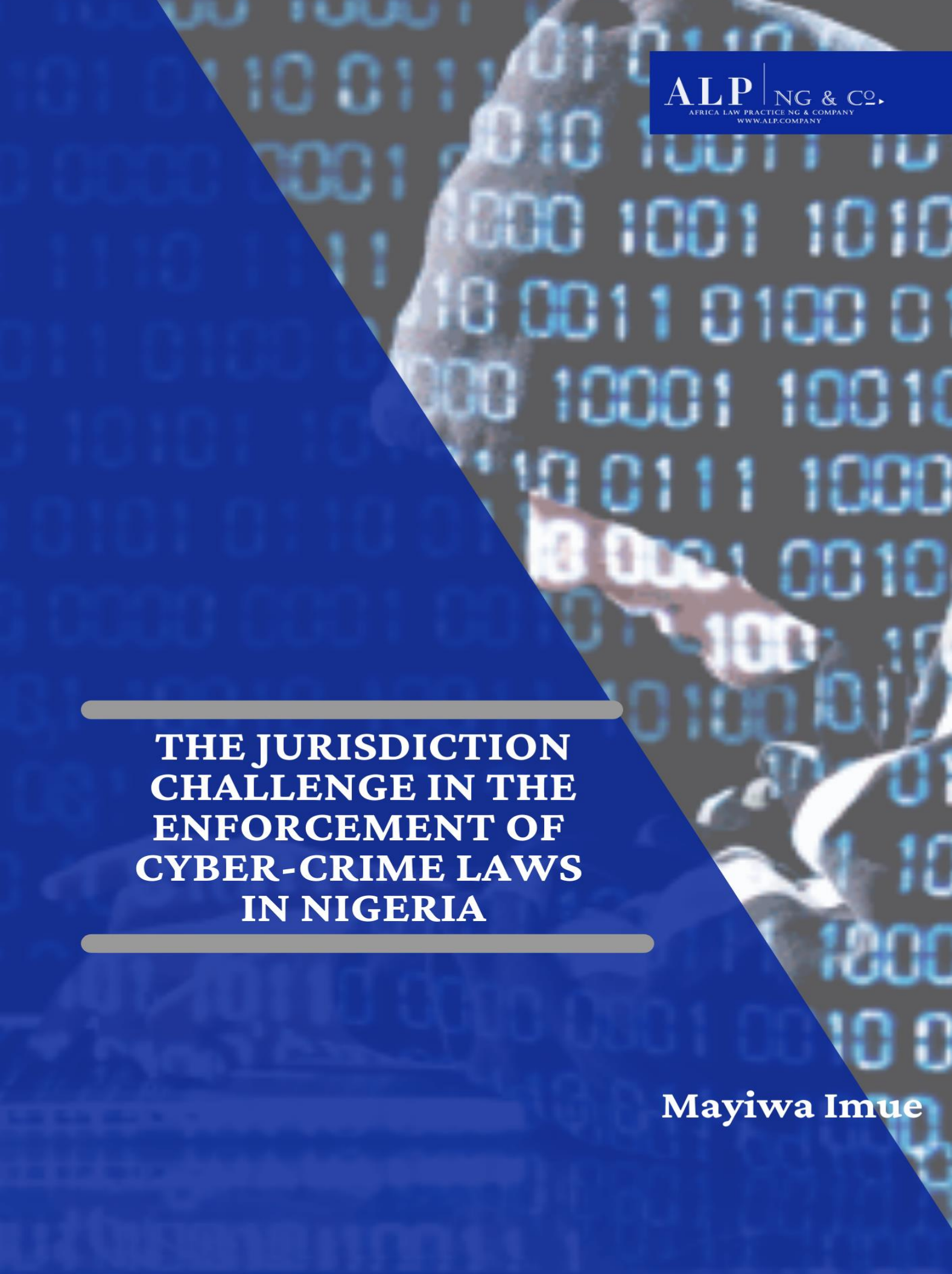

ALP | NG & Co.
AFRICA LAW PRACTICE NG & COMPANY
WWW.ALP.COMPANY

THE JURISDICTION CHALLENGE IN THE ENFORCEMENT OF CYBER-CRIME LAWS IN NIGERIA

Mayiwa Imue

Introduction

This paper examines the factors that militate against the effective enforcement of Cybercrime legislation in Nigeria with an emphasis on the jurisdictional challenges encountered in the enforcement of such legislation.

The fact that cybercrime requires little or no investment to start and can be carried out in various locations without any iota of geographical constraints are largely responsible for the rapid increase in cybercrimes. The estimated global losses to cybercrime in 2018 was $600 billion and in 2020 the number drastically increased to $1trillion[1]. The sudden increase in cybercrime in 2020 was as a result of the outbreak of the COVID-19 pandemic, which drove the world into the internet space more rapidly than we could have envisaged.

Definition of Cybercrime

The Black's Law Dictionary defines cybercrime as *a crime involving the use of computer, such as sabotaging or stealing electronically stored data.*

Legal Framework for Cybercrime in Nigeria

The most prevalent cybercrimes in Nigeria which are codified into the Cybercrimes (Prohibition, Prevention, etc.) Act 2015[2] (the Act) are hacking, software piracy, pornography, viruses and worms spamming, website cloning, credit card or ATM fraud, denial of service attack, virus dissemination, phishing, cyber plagiarism, cyber stalking, cyber defamation, cyber terrorism.

Apart from the Act, there are several other legislations which deal with cybercrimes in Nigeria, including the Criminal Code Act[3], Money Laundering (Prohibition) Act (MLA) 2011[4], Advance Fee Fraud Act[5], Nigeria Data Protection Regulation 2019 and Nigerian Communications Act (NCA) 2003[6]. However, the focus of this article is the Act which is established primarily to curb cybercrimes in Nigeria.

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ("the Act")

The Act has the objective of providing an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Act also seeks to promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights. The Act establishes the Nigerian Cybercrime Working Group (NCWG) for the effective enforcement of the Act. The two major prosecuting bodies under the Act are the Economic and Financial Crimes Commission (EFCC) and the Federal Ministry of Justice.

Curbing Cybercrimes in several Industries in Nigeria

- **Telecommunications -** The Cybercrime Act sets out the duties of telecommunication service providers in record retention and data protection. Under the Act[7], a relevant authority or a law enforcement agency can request for a service provider to (a) keep any traffic data, subscriber
- information, and content or non-content information; or (b) release any information it has stored. The Act further makes it a duty on service providers to release traffic data and subscriber information[8] but

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[2] The Cybercrimes (prohibition, prevention, etc.) Act 2015
[3] section 419 Criminal Code Act
[4] Section 2 Money Laundering (Prohibition) Act (MLA) 2011
[5] Section 1 Advance Fee Fraud and Other Related Offences Act 2006
[6] Section 146 of Nigerian Communications Act 2003
[7] Section 38(2) of Cybercrimes (prohibition, prevention, etc) Act 2015
[8] Ibid., s 38(3).

restricts the use of this information to legitimate purposes only[9].

- **Banks and other Financial Institutions -** The Nigeria Electronic Fraud Forum (NEFF)[10] which is in conjunction with the Central Bank of Nigeria and Nigeria Bankers Committee has the sole aim of monitoring online bank transactions by sharing fraud data among banks and formulating risk management strategies to secure e-payment transactions. NEFF has created an organized structure to safeguard the integrity of e-payment channels and ensures consumers are protected from cyberattacks through electronic payments.
  On a related note, the Nigeria Deposit Insurance Corporation (NDIC) controls the activities of financial institutions in Nigeria. NDIC has a supervisory power over insured financial institutions or banks to request for information when required[11].

The Issue of Jurisdiction

Jurisdiction is so radical that it forms the basis of any adjudication and goes into the roots of any matter before the courts. If a court lacks jurisdiction, it also lacks the necessary competence to try the case. The Court of Appeal stated that "Jurisdiction is the life wire of a Court as no Court can entertain a matter where it lacks jurisdiction."[12]

The critical question in relation to cybercrimes is whether it can be said that cybercrime offences lack locus delicti or whether the offences could be said to have multiple locus delicti because the cases are multijurisdictional.

In most cases, extradition is seen as an option of solving the jurisdiction challenge, but there must be an existence of extradition treaty between states to automatically return cybercriminals for trial[13]. And in such case, the dual criminality principle needs to be fulfilled. This simply means that before a suspect can be validly extradited, both the requested state and state of domicile of the criminal must ensure that the alleged offence is punishable in their respective states.

In Nigeria, the Federal High Court has jurisdiction to try offences under the Cybercrime Act (the "Act")[14] and such offences are extraditable under the Extradition Act[15].

Section 52 of the Act on its part provides as follows:

> *The Attorney General of the Federation may request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences under this Act and may authorize or participate in any joint investigation or cooperation carried out for detecting, preventing, responding and prosecuting any offence under this Act. And such joint investigation or cooperation may be carried out* ***whether or not*** *any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. Furthermore, the Attorney-General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of an investigation, if such information will assist in the investigation of an offence or the apprehension of an offender under this Act*[16].

This section clarifies the issue of existing treaties between states for extradition to be effective. The absence of a treaty will not hinder the enforcement of the law where there is an occurrence of cybercrime. Although under international law, no instrument imposes on sovereign nations an obligation to automatically extradite cybercriminals,

[9] Ibid., s 38(4).
[10] https://www.cbn.gov.ng/neff/about.asp
[11] Sections 27 of Nigeria Deposit Insurance Corporation Act 2006
[12] Dairo v. UNION BANK OF NIGERIA PLC [2007] 16 NWLR (PT. 1059) 99
[13] Section 1 and 2 of Extradition Act, CAP E25, Volume 6, Laws of the Federation of Nigeria, 2004
[14] Section 50 Cybercrimes (prohibition, prevention, etc) Act 2015
[15] Extradition Act, CAP E25, Volume 6, Laws of the Federation of Nigeria, 2004
[16] Section 52 Cybercrimes (prohibition, prevention, etc) Act 2015

but with the aid of cooperation between states, this will enhance the prosecution of the cybercriminal.

The recent collaboration between the Federal Bureau of Investigation (FBI) and Economic and Financial Crimes Commission (EFCC) under the "operation rewired" in 2019 recorded tremendous success in apprehending cyber criminals and recovered the sum of $251,000 from 281 arrests recorded in the US and overseas, including 167 in Nigeria[17].

Another collaboration which has yielded positive results is a joint effort of International Criminal Police Organization (INTERPOL), Group-IB and Nigeria Police Force cybercrime Investigation, where three suspects have been arrested in Lagos which are believed to have compromised government and private sector companies in more than 150 countries since 2017[18].

For an investigation of cybercrime, the NDIC introduced a 24-hour toll-free telephone and a Complaint Unit in its Bank Examination Department and Special Insured Institutions Department (SIID) to enable bank customers and the general public report any financial abuses for investigation and possible resolution in cases where there are problems ranging from arbitrary interest charges, account balances manipulation and cybercrime issues in Nigeria.

Bridging the Jurisdiction Gap and access to Information

The signing of the West African Police Information System (WAPIS) Programme which was implemented by INTERPOL, will create an overall development of a regional platform for stronger criminal data exchange and access to Interpol communication system[19]. The current partnership of the INTERPOL with the Organisation for Economic Co-operation and Development will also create an interface for members of both organizations in curbing the continued increase in cybercrime.

The recent extension of information by INTERPOL to EFCC in the information platform codenamed 1p-247 will enhance the global police communications system to connect with law enforcement agencies in all the 194 INTERPOL member countries.[20] This has provided direct access for EFCC to obtain information about criminal activities across the world. With this development, countries will have quick and collaborative response to cybercrimes.

Conclusion

The seamless continuous communication and cooperation between INTERPOL and its Regional/State counterparts, as well as the domestication of treaties on extradition, will help minimize the jurisdictional challenge that has characterized the enforcement of cyber-crimes. Meanwhile, the Nigerian government should normalize data sharing between government agencies and key private sector players in order to strengthen the law enforcement agencies. However, individuals and organizations involved in data control or processing must ensure that the data security measures for protection of their cyber space are created, and such measures must be updated periodically to respond to emerging threats.

Author

Mayiwa Imue
Associate
mimue@alp.company

[17] efccnigeria.org
[18] Interpol.int
[19]https://www.interpol.int/en/News-and-Events/News/2019/Nigeria-and-INTERPOL-formalize-West-African-Police-Information-System-cooperation
[20]https://www.efccnigeria.org/efcc/news/5747-interpol-extends-specialized-platform-to-efcc