A CRITICAL EXPOSITION OF THE NIGERIAN CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015

F. E. Eboibi*

Abstract

The Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act, 2015(the Act) is the first Nigerian legislation that regulates the activities of persons online. It is a swift legislative response to the ever-increasing technological challenges, especially the perpetuation of crime in cyberspace. Although the development of information and communication technology has paved the way for its positive impact in society, it has engineered the perpetuation and proliferation of heinous crimes through the internet. Consequently, most nations having recognized the perpetration of crimes through the internet have enacted Laws to regulate the conduct of persons in cyberspace. It is in this regard that the Nigerian Act expressly set out what constitutes a cybercrime offence and the punishment for any cyber-related offence. Despite the laudable nature of the Act, it raises many concerns concerning some of the provisions. Hence, this paper endeavours a critical analysis of the provisions of the Act. It considers the general division of the Act into various parts. The tabulation of offences and ascribed punishments created under the Act for ease of reference and key

* Ph.D, Faculty of Law, Niger Delta University, Bayelsa

provisions that might constitute a stumbling block to the implementation of the Act and possible conflicts with other Acts of the National Assembly are considered.

Key-Words: Cybercrime Law, Cyberspace, Cybercrime offence, Cybercrime punishment, Nigeria.

Introduction

The growth of technology and its attendant effect on the global society cannot be undermined by the mere fact that laws exist to regulate the activities of citizens in our country. This is borne out of the fact that with the growth of internet facilities and the liberalization of cyberspace comes an increase in the rate of cybercrime perpetuation in our society, which has posed difficult task on our law enforcement agencies.[1] Today, technological devices like mobile phones, laptops, desktop computers, the internet, websites, and palm pilots are being used to commit crimes.[2] It is axiomatic to assert that cybercriminals in Nigeria, just as in all other countries, make illegal use of the internet to trap the ever gullible victims who cut across all professions, the legal profession not exempted.[3] These acts of cybercrime have placed the entire society at risk, which, if not checkmated, has the potential of creating social distrust, the political backlash, and economic sabotage.

---

[1] Michael Kunz, Patrick Wilson, 'Computer Crime and Computer Fraud; Report to the Montgomery County Criminal Justice Coordinating Commission, 2004' <https://www.montgomerycountymd.gov/cjcc/resources/files/computer_crime_study.pdf> accessed 15 December 2019.

[2] *Ibid*.

[3] F.E. Eboibi 'Legal Approach to Computers' (2014) 13 *Nigerian Law and Practice Journal*, 33-34; F.E Eboibi, 'Chapter 2 – Introduction to Law and Cybercrime' in F.E Eboibi(ed), *Handbook on Nigerian Cybercrime Law*, (Justice Jeco Printing & Publishing Global, Benin, 2018), 9-245.

The most worrisome aspect of the perpetuation of cybercrime in the peculiar case of Nigeria is that it has raised the countries negative indexes as regards its relationship in the committee of Nations.[4] Due to the technical nature of the crime, law enforcement agents are faced with the difficult task of determining what crimes are cybercrimes and the necessary knowledge and skill to carry out investigation properly.[5] Consequently, globally countries are expected to update and enact cybercrime legislation that proscribes cyber-related crimes and put in place suitable punishments for cybercrime offences. This is even more germane because, with the development of information and communication technologies, these crimes would be committed more often by cybercriminals. Hence, the knowledge of what qualifies as a cybercrime or cybercrime offence by law enforcement agents, civilians, or the general public, stakeholders of the criminal justice system cannot be undermined in order to curtail the impact these crimes can pose negatively.[6] In this regard, has the Nigerian government put in place any legislation to prohibit the perpetration of cybercrimes in cyberspace? If yes, are there provisions that are capable of militating against the enforcement of cybercrimes in Nigeria?

Based on the preceding premise, several committees were set up to take a legal, cum holistic view on the cybercrime-related issues by the Nigerian government. The result of this development was the enactment of the Cybercrimes (Prohibition, Protection, Etc) Act,

---

[4] Ibid; F.E Eboibi, 'A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015' (2017) 33(5) *Computer Law and Security Review,* 700 - 717

[5] F.E Eboibi, 'Cybercrime in a Technological Era: Definitional Controversies and Nigeria's Historical Antecedents' (2017) 2(1) *NSUK Law Commentaries,* 43-64.

[6] Michael Kunz & Patrick Wilson, (n.1).

2015. The Act expressly sets out what constitutes a cybercrime or cybercrime offence and also states in detail the punishment for any cyber-related offence. Although the Act did not expressly define the concept of cybercrime, the title of the legislation merely encompasses the word "cybercrimes."[7] The interpretation section is also not helpful as it did not offer any meaning to the concept of cybercrime.[8] This deliberate omission may be attributable to the absence of an acceptable universal meaning of the concept of cybercrime. This is further compounded by its deliberate omission in both domestic and international cybercrime legislations. Specifically, the Council of Europe Cybercrime Convention, African Union Convention, and Arab States Convention did not ascribe any meaning to cybercrime.[9] Honourable Justice I.N Buba acknowledged this fact in *Solomon Okedara v. The Attorney General of the Federation,* when he stated that "…the applicant has to come to terms with the realities of life in the 21st Century and the use of cyberspace to commit offences. Indeed, cybercrime itself has not or has never had a single acceptable definition."[10] What the Nigerian Cybercrime legislation has done is to "consider a collection of acts or conduct, rather than one single act and consequently, described the basic content of the term by a non-exhaustive list of acts that constitute cybercrime."[11]

Nevertheless, the concept of cybercrime is generally referred to as crimes committed where computers or networks are a tool, target,

---

7 *Cybercrimes* (Prohibition, Prevention Etc) Act, 2015, emphasis added

8 *Ibid*. s.58.

9 F.E Eboibi, (n.5); F.E Eboibi, (n.3).

10 Unreported – Suit No: FHC/L/CS/937/2017, Judgment delivered on Thursday 7 December 2017, Federal High Court, Lagos Judicial Division, Holden at Lagos, at 34.

11 F.E Eboibi, (n.5); F.E Eboibi,(n.3).

or a place of criminal activity.[12] It is a "generic term that refers to all criminal activities done using the medium of computers, the internet, cyberspace, and the worldwide web."[13] When used comprehensively, "cybercrime means an unlawful act or default involving the use of or relating to computers, computer networks or virtual reality, especially the internet, which is an offence against the public and render the person guilty of the act liable to legal punishment. It does mean a criminal offence perpetrated on the web, a violation of cybercrime law or law on the internet which act is harmful in itself, or its outcome also renders the cybercriminal liable to some kind of punishment."[14]

To put the Act in a proper perspective, this paper is an attempt to examine the provisions from a critical perspective by initially considering the general division of the Act into various parts. After that, the offences and the punishments created under the Act are tabulated for ease of reference, key provisions that might constitute a clog to the enforcement of the Act, and possible conflicts with other Acts of the National Assembly are considered. In the final analysis, deductions based on the discourse is made and consequent recommendations where necessary.

Summary of the Cybercrimes (Prohibition, Prevention Etc) Act, 2015

The Act is the Nigerian first comprehensive law on cybercrime and computer-related crimes. The proliferation of cybercrime and the quest by the Nigerian government to curtail its negative implications partly influenced the enactment of the Act. In

[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid*.

fulfillment of its legislative duties, the Nigerian National Assembly passed the Act into Law on 5 May 2015. The Act comprises 59 sections, 8 parts, and two schedules. The preamble to the Act shows that it is "an Act to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes; and for related matters."[15] To properly appreciate the intendment of the Act, the section below highlights the various parts and provisions of the Act.

Part I: Object and Application

The first part of the Act christened PART I contains Sections 1 and 2 of the Act. Section 1 states the objectives of the Act: It is geared towards "an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria."[16] Moreover, the protection of Nigerian critical infrastructure as it relates to information is one of the objectives of the Act.[17] Section 58 of the Act defines critical infrastructure as "systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country."[18] Also, the promotion of cyber security and ensuring that "computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights" are protected in the Nigerian polity underscores one of the objectives of the Act.[19]

---

[15] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, preamble
[16] *Ibid*., s.1(a)
[17] *Ibid*,. s.1(b)
[18] *Ibid*., s.58
[19] *Ibid*., s.1(c)

Section 2 of the Act provides for the applicability of the Act throughout the Federal Republic of Nigeria. The transboundary nature of the cyberspace may have influenced the drafters of the Act towards maintaining a national application of the Act. This works to the exclusion of States House of Assembly in validly making any Law to regulate the activities or conducts of persons online or cybercrime in a State. Section 2 seems to have reinforced the doctrine of covering the field enshrined in Section 4(5) of the Constitution of the Federal Republic of Nigeria 1999 (as amended). This implies that where a law enacted by a State House of Assembly is inconsistent with any law validly enacted by the National Assembly, the law so enacted by the National Assembly shall prevail.[20]

Part II: Protection of Critical National Information Infrastructure

This is the second part of the Act, and the same is titled PART II. This part contains two sections: Sections 3 and 4, which provides for the protection of Critical National Information Infrastructure. The protection provided here is to make sure that critical infrastructures are not tampered with by third parties and cybercriminals. Section 58 of the Act, as stated earlier in this work, defines critical infrastructure. Specifically, section 3(1) of the Act empowers the President of the Federal Republic of Nigeria based on the recommendation of the National Security Adviser by order published in the Federal Gazette to designate computer systems as Critical National Information infrastructure.[21] Where an order is made by the President pursuant to section 3(1) of the Act,

---

[20] *A.G. Federation v. A.G. Lagos State* (2013) LPELR-20974(SC) pp.178-179 paras G-F

[21] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.3(1).

subsection 2 empowers the President to set out the minimum standards, guidelines, and rules and procedure in respect of the Critical National Information Infrastructure.[22]

Part III: Offences and Penalties

The part comprises sections 5 to 36 of the Act. It provides for general offences and penalties by setting out the offences and the accompanied punishment where it is in breach by persons, individuals, and corporate organizations. Generally, this work identifies about seventy offences and penalties under the Act. Section 3 of this work sets out in detail the said offences and the punishment prescribed therein.

Part IV: Duties of Financial Institutions and Service Providers

Part IV of the Act encapsulates sections 37 to 40 of the Act. Section 37 of the Act saddles with financial institutions the responsibility to verify the identity of their customers before the issuance of any form of a card or electronic device.[23] A financial institution, according to the Act, is "any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities…"[24] Interestingly, Section 37(3) saddles financial institutions with the responsibility of reversing within 72 hours any unauthorized debit made on account of a customer. It is a cybercrime offence for any financial institution refusal to do so. This provision is generally practiced in breach by financial institutions in Nigeria.[25] This may be a result of poor orientation as

---

[22] *Ibid*., s.3(2).
[23] *Ibid*., s.37(1)(a) &(b).
[24] *Ibid*., s.58.
[25] *Kume Bridget Ashiemar v. Guarantee Trust Bank Plc & United Bank for Africa Plc* (Unreported), Suit No: MHC/198/2014 – Judgment delivered by

to the applicability of the Act to financial transactions. This provision seems to have provided for the regulation of the operations of Banks and Financial Institutions despite their operations already being governed by the Central Bank of Nigeria Act[26] and the Banks and Other Financial Institutions Act (BOFIA).[27]

Section 38, 39 and 40 of the Act provides for the duties of service providers. According to the Act, Service Provider mean "any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks and any entity that processes or stores computer data on behalf of such communication service or users of such service."[28] By virtue of the Act, service providers are duty-bound to retain all subscriber information for 2 years. They shall only release such information to regulatory agencies subject to an individual's right to privacy under the Nigerian Constitution.[29] However, law enforcement agents' access to such information for purposes of criminal investigation is subject to the discretionary order of a judge.[30] Failure to provide information upon request by a law enforcement agent from a service provider to enhance cybercrime investigation under the Act constitutes an offence.[31] Again, despite extensive regulation of

---

Hon. Justice T.A Igoche on 24 May 2018 of the High Court of Justice, Benue Judicial Division, Holden at Makurdi.

26 Cap C4, Laws of the Federation of Nigeria, 2004

27 Cap B3, Laws of the Federation of Nigeria, 2004

28 The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.58(a)&(b)

29 *Ibid*., s.38.

30 *Ibid*., s.39.

31 *Ibid*., s.40.

service providers by the Nigerian Communications Act, 2003 this Act seems to have usurped the powers of the NCC in this respect.[32]

Part V: Administration and Enforcement

This fifth Part comprises of sections 41 to 44 of the Act. Section 41(1) of the Act automatically makes the office of the National Security Adviser (ONSA) the body to coordinate all security and enforcement agencies under the Act. Unfortunately, no particular agency is mentioned throughout the Act. It begs the question of which particular agency or agencies is/are subject to the coordination of the ONSA. Furthermore, the subsection empowers the ONSA with other onerous tasks under the Act. For instance, the ONSA is mandated to give support to all relevant security, law enforcement agencies, intelligence, and military services to ensure the prevention and combating of cybercrimes in Nigeria.[33] Again, what nature of support is expected from the ONSA that is a political position and theoretical established cybercrime knowledge and know-how. Except this duty would be read together with the duty to provide or establish and maintain a National Computer Emergency Response Team (CERT) and the National Computer Forensic Laboratory.[34] Although the ONSA has established CERT, its effectiveness, and efficiency when compared to what is obtainable under the operations of the US CERT and UK CERT is in serious doubt.[35] Also, the ONSA is empowered to ensure that

---

[32] NCC Act 2003

[33] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.41(1)(a)

[34] *Ibid*., s.41(1)(c)&(d).

[35] Nigeria Computer emergency Response Team, ngcert, <https://www.cert.gov.ng/news-and-events> accessed 17 December 2018; Compare the online activities of ngCERT - <https://www.cert.gov.ng/news-and-events> on one hand and US-CERT and UK-CERT on the other hand at <https://www.us-cert.gov/ & http://www.ukcert.org.uk/>, accessed 15 May 2018.

Nigeria is involved in international cyber security cooperation to enhance the integration of Nigeria into the global framework on cyber security.[36]

Section 41(2) of the Act gives the nod to the Attorney General (AG) of the Federation by empowering him/her to ensure that Nigeria's legal framework on cybercrime and cyber security meets regional and international standards, while also maintaining international cooperation for cybercrime prevention and curtailment.[37] For the capacity building amongst personnel involved in the prohibition, prevention, detection, investigation, and prosecution of cybercrimes, subsection 3 also empowers the ONSA to collaborate with other law enforcement agencies to put in place training programs.[38] The implementation of this subsection is very germane to the fight against cybercrime in Nigeria, considering the lack of technological know-how and forensic skills of most cybercrime investigators and prosecutors in Nigeria.[39]

Section 42 of the Act provides for the establishment of the Cybercrime Advisory Council. The Nigerian government has since inaugurated the Council. Section 43 of the Act outlines the functions of the Council to include the creation of an enabling

---

36 *Ibid*., s.41(1)(g).

37 *Ibid*., s.41(2)

38 *Ibid*., s.41(3)

39 Ikenga K. E. Oraegbunam, 'The Nigeria Police and Problems of Cybercrime Investigation: Need for Adequate Training', 19 – 22, <https://www.academia.edu/26360705/The_Nigeria_Police_and_Problems_of_Cybercrime_ Investigation_Need_for_Adequate_Training1?auto=download> accessed 16 April 2019; S.O Abu, O.M Lateef and J. Echobu 'Determinants of Cybercrime Investigation in Nigeria' (2018) 2(2) *Accounting & Taxation Review*, 2-12,

environment for ideas, knowledge, experience, intelligence, and information to be shared regularly and make appropriate recommendations and advice for combating and preventing cybercrime in Nigeria. Despite the existence of this institution, cybercrime's commission is proliferating daily in Nigeria. This may arguably be attributed to the Council's lack of implementation of its assigned functions. Again, the Council is empowered to put in place programs for the award of grants to institutions of higher education to establish Cyber security Research Centers.

Nevertheless, no meaningful achievement has been recorded in this regard. Cyber security or cybercrime is not being taught in most institutions of higher learning. The few institutions that are undergoing research in this area are stagnated due to a lack of funding. The Faculty of Law, Niger Delta University, offers Cybercrime Law at the undergraduate level and Cybercrime Law and Digital Forensics at the Post-Graduate level. The necessary funding to actualize both teaching tools and appropriate research is lacking. The quest to curtail and prevent cybercrime must, as a matter of urgency, be channeled towards research to identify the recent trends of cybercriminals and how they can be detected to enhance cyber security measures.

National Cyber Security fund is established by section 44 of the Act under the management of the Central Bank of Nigeria (CBN) and the ONSA where monies shall be paid into.[40] The implication is that internet service providers, GSM service providers, and all telecommunication companies, banks, and other financial institutions, insurance companies, and the Nigerian Stock Exchange are mandated to compulsorily contribute a levy of 0.005

[40] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.44(1) & (2).

of all electronic transactions to the Fund domiciled in CBN.[41] The affected organizations have risen against the aforementioned levy imposed by the Act and concerns about its likely impact on the business industry.[42] Moreover, a fundamental flaw about the levy is that the Act did not specify the nature of punishment that would be meted out against defaulters. In the absence of that, the subsection would likely be observed more in breach. More worrisome is the fact that despite the commencement of the Act since 15 May 2015, the CBN only recently sent out circulars to the affected organizations pursuant to the subsection reminding them of their duty to remit to the

Fund.[43] Other areas where the fund would be generated for the National Cyber Security fund include grants and assistance from both domestic and international agencies, gifts, endowments, and other contributions by individuals and agencies.[44]

---

[41] *Ibid.,* second schedule; s.44(2)(a)

[42] Sunnews Online, 'ATCON kicks against CBN's 0.005% levy on electronic transactions,' 23 May 2018, <https://sunnewsonline.com/atcon-kicks-against-cbns-0-005-levy-on-electronic-transactions/> accessed 20 December 2018; Jackson, Etti & Edu, Is the Cyber security Levy a Veiled Cyber tax*?* <https://www.jacksonettiandedu. com/wp-content/uploads/2018/07/IS-THE-CYBERSECURITY-LEVY-A-VEILED-CYBERTAX.pdf> accessed 20 December 2018.

[43] Central Bank of Nigeria, Banking and Payments System Department, BPS/DIR/GEN/CIR/05/008, Circular on compliance with the Cybercrime(Prohibition, Prevention Etc) Act 2015: Collection and Remittance of Levy for the National Cyber security Fund. <https://www.cbn.gov.ng/Out/2018/BPSD/Circular%20on%20Compliance%20with% 20the%20Cybercrime%20(prohibition,prevention,%20etc.).pdf> accessed 20 December 2018; Onome Ohwovoriole, CBN to begin collection of Cyber security levy this month', 5 July 2018, <https://nairametrics.com/cbn-releases-guidelines-for-collection-of-cyber-security-levy/> accessed 20 December 2018.

[44] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.44(2)(b)&(c).

Part VI: Arrest, Search, Seizure, and Prosecution

Part VI of the Act encapsulates sections 45 to 49. Section 45 enjoins all law enforcement agents who wish to obtain any electronic evidence pursuant to cybercrime investigation for offences provided under the Act to seek the order of the Court through an *exparte* application made to a Judge in Chambers for the issuance of the warrant.[45] The question that seems unanswered by the subsection is the particular Court that should entertain such an application. The way the provision is couched, the subjective interpretation would conclude that any Court presided by a Judge can issue the warrant. Other provisions of the Act do not support this interpretation. For instance, section 50 of the Act equips the Federal High Court with exclusive jurisdiction to entertain matters under this Act. It follows that all issues concerning offences under investigation and prosecution pursuant to the Act, including the issuance of a warrant, is the exclusive preserve of the Federal High Court Judge.

The implication of the foregoing is that stop and search of premises and conveyance, computer and electronic devices, and the use of technology to decode evidence against suspected perpetrators of cybercrimes must be carried out by law enforcement agents subject to obtaining the necessary warrant from the Federal High Court Judge.[46] When juxtaposed against the background of realities in the Nigerian polity where innocent and suspected persons' mobile phones and computer devices are searched at random in the guise of looking for cybercrime incriminating evidence by law enforcement agents shows the observance of the subsection in breach.

---

[45] *Ibid*., s.45(1).
[46] *Ibid*., s.45(2).

Section 46 of the Act makes the deliberate obstruction of a law enforcement agent in the course of carrying out his duties under the Act a criminal offence.[47] This section is likely to be abused by law enforcement agents because what can amount to an obstruction under the Act is not stated. It gives room for subjective interpretation. However, subsection (b) gives a clearer picture of the intendment of the drafters of the Act, where failure to comply with any lawful inquiry or request made by a law enforcement agency based on the provisions of the Act is seen as a criminal offence.

Section 47(1) of the Act empowers relevant law enforcement agencies to prosecute perpetrators of cybercrime. This power of prosecution is, however, subject to the powers of the A.G of the Federation. Again, how can "relevant law enforcement agencies" be determined for them to be equipped to prosecute cybercrime matters under the Act? This provision gives the impression that any law enforcement agency that claims to be relevant can prosecute perpetrators of cybercrime. Based on the peculiarity of cybercrime, there is a need for a specific agency to be empowered to prosecute cybercrime in Nigeria. It is a technology-based crime; hence not every agency has the technological know-how to prosecute the crime. However, with respect to offences mentioned in sections 19 and 21 of the Act, the approval of the A.G must be sought before any prosecution is undertaken.[48]

Section 48 of the Act empowers the Court upon the conviction of a defendant to order the forfeiture of the proceeds of the crime to the Federal Republic of Nigeria whether the proceeds are domiciled in

---

[47] *Ibid*., s.46(a).
[48] *Ibid.,* s.47(2).

Nigeria or foreign country subject to the applicable rules. On the other hand, section 49 of the Act gives the Court a discretionary power to make an order for a convicted defendant to restitute or compensate the victim of the offence with respect to lost monies and properties.

Part VII: Jurisdiction and International Co-operation

Part VII of the Act contains sections 50 to 56. Jurisdiction, which is the power or authority of a Court of competent jurisdiction to entertain a matter is vested on the Federal High Court to entertain cybercrime matters under the Act by virtue of section 50. This is irrespective of where the cybercrime offence is committed "in Nigeria, in a ship or aircraft registered in Nigeria, 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 was committed, or outside Nigeria where the victim of the offence is a citizen or the alleged offender is in Nigeria and not extradited to any other country for prosecution."[49]

Section 51 of the Act states that offences provided under the Act are subject to extradition under the Extradition Act.[50] Section 1 of the Extradition Act provides that "where a treaty or other agreement has been made by Nigeria with any other country for the surrender by each country to the other, of any persons wanted for prosecution or punishment, the National Council of Ministers may by order published in the Federal Gazette apply this Act to that country."[51] This implies that any Country Nigeria enters a treaty

[49] *Ibid*., s.50(1)(a)-(d).
[50] E25, Laws of the Federation of Nigeria, 2004.
[51] Extradition Act, s.1.

with, in this regard, will enhance international co-operation in the fight against cybercrime.

Section 52 of the Act gives A.G of the Federation the power to request for any assistance whatsoever from any agency or authority of a foreign state for investigation and prosecution of cybercrime offences under the Act. This will enhance joint investigation between Nigerian law enforcement agents and foreign counterparts, especially where cybercrime is a borderless crime. Section 53 of the Act allows the use of evidence requested from any foreign country in the course of proceedings in the Nigerian Courts provided such evidence is authenticated or certified by a judge, magistrate or Justice of Peace, or by the seal of a ministry or department of the Government of a foreign state. This provision seems to have limited those who can certify foreign evidence contrary to section 106(h) of the Evidence Act 2011.[52] Similarly, the Act allows foreign States to request evidence but set out modalities for such a request to be honoured. The request must be in writing, dated, and signed by the person requesting or on his behalf. Facsimile or other electronic means is acceptable but should include the name of the authority in charge of the investigation or prosecution, description of the subject matter, evidence, the information sought and the purpose for which they are sought.[53]

Section 55 of the Act provides for expedited preservation of computer data. Section 56 of the Act mandates the ONSA for the purpose of international cooperation to make available a contact point twenty-four hours a day. It provides that the contact point

[52] Section 106(h) includes certification by a notary public or a consul or diplomatic agent, and its admission shall be upon proof of the character of the document according to the Law of the foreign country.
[53] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.54(1)&(2).

shall be reached by other countries of other contact points in accordance with agreements, treaties, or conventions.

Part VII: Miscellaneous

Part VIII comprises of sections 57 to 59 of the Act. Section 57 of the Act mandates the A.G to put in place rules or regulations for the efficient implementation of the provisions of the Act where necessary. By this provision, the A.G can arguably make rules and regulations to circumvent identified pitfalls of the Act for effective enforcement of the Act. The definition section and citation are contained in sections 58 and 59, respectively. The members of the Cybercrime Advisory Council are listed in the First Schedule to the Act, while the Second schedule to the Act lists the businesses which Section 44(2)(a) of the Act applies.

Offences and Punishments under the Act

It should be understood that part three of the Act create offences and penalties or punishments. This aspect of the discourse centers on the offences and their penalties referred to in 2.3 above.

S/N	OFFENCE	SECTION	PUNISHMENT/ PENALTY
1	Unlawful and unauthorized access of computer systems or networks for fraudulently obtaining of data vital to national security	Section 6 (1)	Imprisonment for a term of not more than 5 years Fine N5million or both
2	Unlawful and authorized access of computer systems or networks for fraudulently obtaining computer data, program, commercial or industrial secrets or classified information	Section 6 (2)	Imprisonment for a term of not more than 7 years or to a fine of not more than N7 million or both.
3	Use of any device to avoid	Section 6	Imprisonment for a term

	detection for the purpose of committing any of the above offences	(3)	of not more than 7 years or to a fine of not more than N7 million or both
4	Password trafficking	Section 6 (4)	Imprisonment for a term of not more than 3 years or fine of not more than N7 million or both.
5	Electronic or online fraud with the use of a cybercafé	Section 7(2)	Imprisonment for a term of 3 years or fine of N1 million or both.
6	Connivance by owners of cybercafé with electronic or online fraudsters	Section 7(3)	Imprisonment for a term of 3 years or fine of N2 million or both.
7	Unlawful interference with a computer system	Section 8 and Section 16 (3)	Imprisonment for a term of not more than 2 years or to a fine of not more than N5 million or both
8	Unlawful destruction or abortion of emails or electronic process through which money or other valuable information is being conveyed	Section 9	Penalty: First conviction – Imprisonment for a term of 7 years Subsequent convictions: Imprisonment for a term of 14 years
9	Obtaining electronic messages (emails, credit and debit cards information, facsimile messages etc.) by false pretenses	Section 12 (2)	Imprisonment for a term of 2 years or to a fine of not more than N1 million or both.
10	Electronic forgery	Section 13	Imprisonment for a term of not less than 3 years or to a fine of not less than N7 million or both.
11	Unlawful interference with a computer system causing loss of property	Section 14 (1)	Imprisonment for a term of not less than 3 years or to a fine of not less than N7 million or both.
12	Fraudulent misrepresentation by electronic means/ Internet fraud	Section 14 (2)	Imprisonment for a term of not less than 5 years or to a fine of not less than N10 million or

			both.
13	Fraudulent manipulation of electronic payment devices	Section 14 (4) & (6)	Imprisonment for a term of not more than 7 years and shall forfeit proprietary interest in the stolen money or property to the bank, financial institution or customer.
14	Fraudulent diversion of emails by bankers	Section 14 (5)	Imprisonment of not more than 5 years or fine of not more than N7 million or both
15	Connivance by bank/banker to commit electronic fraud	Section 14 (7)	Imprisonment for a term of not more than 7 years and shall refund the stolen money or forfeit any property to which it has been converted to the bank or customer.
16	Theft of a bank or public infrastructure's terminal	Section 15 (1)	Imprisonment for a term of 3 years or to a fine of N1 million or both.
17	Theft of an ATM	Section 15 (2)	Imprisonment for a term of not more than 7 years or to a fine of not more than N10 million or both and all proceeds of the theft shall be forfeited to the lawful owners of the ATM.
18	Attempted theft of an ATM	Section 15(3)	Imprisonment for a term of not more than 1 year or fine of not more than N1 million or both.
19	Forgery of electronic signature or company's mandate	Section 17 (3)	Imprisonment for a term of not more than 7 years or to a fine of not more than N1 million or both.
20	r terrorism	Section 18	Life Imprisonment
21	Fraudulent issuance of e-	Section 20	Imprisonment for a term

	instructions by bankers		of 7 years.
22	Failure to report cyber threat	Section 21(3)	Denial of Internet services and mandatory fine of N2 million payable into the National Cyber Security Fund.
23	Identity theft by banker	Section 22 (1)	Imprisonment for a term of 7 years or to a fine of N5 million or both
24	Electronic impersonation	Section 22 (2)	Imprisonment for a term of 5 years or to a fine of not more than N7 million or both.
25	Misrepresentation of material facts for the purpose of procuring the issuance of a card or other instrument	Section 22(3)	Imprisonment for a term of not more than 5 years or to a fine of not more than N7 million or both.
26	**PONORGRAPHY RELATED OFFENCES** Unsolicited distribution of pornographic images	Section 23(2)	Imprisonment for a term of 1 year or fine of N250,000.00 or both.
27	Producing, selling, distributing or transmitting child pornography	Section 23(1)	Imprisonment for a term of 10 years or to a fine of not more than N20 million or both.
28	Procuring or possessing child pornography	Section 23(1)	Imprisonment for a term of not more than 5 years or to a fine of not more than N10 million or both.
29	Intentionally proposing, grooming or soliciting to meet a child	Section 23 (3)	Imprisonment for a term of not more than 10 years and to a fine of not more than N15 million.
	Intentionally proposing, grooming or soliciting to meet a child by electronic means for the purpose of engaging in sexual activities with the child where	Section 23 (3)	Imprisonment for a term of not more than 15 years and to a fine of not more than N25 million.

	coercion, inducement, force or threats are used; or where a recognized position of trust, authority or influence over the child is used; or where the vulnerable situation of the child is used; or for the purpose of recruiting, inducing, exposing or causing a child to participate in pornographic performances		
30	Cyber stalking/cyber or electronic libel	Section 24 (1)	Imprisonment for a term of not more than 3 years or to a fine of not more than N7 million or both.
31	Cyber bulling causing fear of death, violence or bodily harm	Section 24 (2)(a)	Imprisonment for a term of 10 years or a minimum fine of N25 million
32	Cyber threat to kidnap or demand for ransom	Section 24(2)(b)	Imprisonment for a term of 10 years or a minimum fine of N25 million.
33	Cyber threat to harm property or reputation	Section 24 (2)(c)	Imprisonment for a term of 5 years or a minimum fine of N15 million.
34	Cyber-squatting	Section 25	Imprisonment for a term of not more than 2 years or to a fine of not more than N5 million or both.
35	**OFFENCES RELATING TO RACE AND XENOPHOBIA** Electronically distributing racist or xenophobic material to the public including threat, insults, etc	Section 26	Imprisonment for a term of not more than 5 years or to a fine of not more than N10 million or both.
36	Attempt to commit an offence under the Act or aiding, abetting, conspiring,	Section 27	Same penalty as provided for the principal offence.

	counseling or procuring another person to commit an offence under the Act		
37	**OFFENCES RELATING TO E-TOOLS** Provision of e-tools and materials required to commit offences under the Act	Section 28 (1) & (4)	Imprisonment for a term of not more than 3 years or to a fine of not more than N7 million or both and imprisonment for a term of not more than 5 years or to a fine of not more than N10 million or both where offence results in loss or damage.
38	Possession of e-tools and materials required to commit offences under the Act with intent to commit an offence	Section 28(2)	Imprisonment for a term of not more than 2 years or to a fine of not more than N5 million or both.
39	Unauthorized disclosure of password, access code or other means of gaining access to any program or data in any computer or network	Section 28(3)	Imprisonment for a term of not more than 2 years or a fine of not more than N5 million or both.
40	Use of any automated means or device or any computer program or software to retrieve, collect and store passwords, access codes or any other means of gaining access to any program, data or database with intent to commit any offence under the Act	Section 28(5)	Imprisonment for a term of not more than 5 years or a to fine of not more than N10 million or both
41	Breach of confidence by service providers	Section 29	Corporate Organization – Fine of N5 million and forfeiture of further equivalent of the monetary value of the loss sustained by the

			consumer. The court may also order that the organization be wound up and all its assets and property be forfeited to the Federal Government. Natural person – Imprisonment for a term of not more than 7 years or to a fine of not more than N5 million or both.
42	Manipulation of ATM machines and POS terminals	Section 30 (1)	Imprisonment for a term of 5 years or to a fine of N5 million or both
43	Conniving to manipulate ATM machines and POS terminals by employees of financial institutions	Section 30(2)	Imprisonment for a term of 7 years without an option of fine.
44	puter Phishing	Section 32 (1)	Imprisonment for a term of 3 years or a fine of N1 million or both.
45	Spamming with intent to disrupt the operations of a computer	Section 32(2)	Imprisonment for a term of 3 years or a fine of N1 million or both.
46	Spread of virus or any malware causing damage to critical information	Section 32(3)	Imprisonment for a term of 3 years or a fine of N1 million or both
47	**ELECTRONIC CARDS RELATED OFFENCES** Fraudulent use of financial electronic cards	Section 33(1)	Imprisonment for a term of not more than 7 years or to a fine of not more than N5 million or both. The convict is also liable to pay in monetary terms the value of loss sustained by the owner of the credit card.
48	Use of counterfeit or unauthorized access device or access device issued to	Section 33(2)	Imprisonment for a term of not more than 7 years or to a fine of not more

	another person resulting in a loss or gain		than N5 million and forfeiture of the advantage or value derived from his act.
49	Theft of an electronic card	Section 33(3)	Imprisonment for a term of not more than 3 years or to a fine of not more than N1 million and is liable to repay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.
50	Retaining possession of stolen or lost electronic card or electronic card delivered by mistake with intent to use, sell or traffic it to a person other than the issuer or cardholder	Section 33(4)	Imprisonment for a term of not more than 3 years or to a fine of not more than N1 million and is liable to pay in monetary terms the value of loss sustained by the cardholder
51	Gaining control over a card as security for a debt with intent to defraud	Section 33 (5)	Imprisonment for a term of not more than 3 years or to a fine of not more than N3 million or both and is liable to pay in monetary terms the value of loss sustained by the card holder or forfeit the assets or goods acquired with the funds from the account or the cardholder.
52	Signing a card without authorization with intent to defraud	Section 33(6)	Imprisonment for a term of not more than 3 years or to a fine of not more than N1 million.

53	Using a card that is obtained fraudulently, forged, expired or without the consent or authorization of the cardholder	Section 33(7)	Imprisonment for a term of not more than 3 years and a fine of not more than N1 million.
54	Furnishing goods or services upon presentation of a card known to be fraudulently or illegally obtained or forged or expired or revoked with intent to defraud	Section 33(8)	Imprisonment for a term of not more than 3 years or a fine of not more than N1 million or both.
55	Failure to furnish goods or services to issuer or cardholder	Section 33(9)	Imprisonment for a term of not more than 3 years or a fine of not more than N1 million or both.
56	Falsely declaring a card transaction record of sale	Section 33(10)	Imprisonment for a term of 3 years and a fine of not more than N500, 000.00.
57	Soliciting a false card transaction record of sale	Section 33(11)	Imprisonment for a term of not more than 3 years or to a fine of not more than N1 million or both.
58	Possession of counterfeit cards or card account numbers of another person	Section 33(12)	Imprisonment for a term of not more than 5 years or to a fine of not more than N3 million or both.
59	Possession, purchase or sale of a card-making equipment with intent that it be used in the manufacture of counterfeit cards	Section 33(13)	Imprisonment for a term of not more than 5 years or to a fine of not more than N7 million or both.
60	Falsification of invoice obtained by use for a card after the invoice has been signed by the cardholder	Section 33(14)	Imprisonment for a term of not more than 3 years or to a fine of not more than N5 million or both.
61	Releasing list of cardholders and their addresses and account numbers by an institution	Section 33(15)	A fine of N10 million

	without the prior written permission of the cardholders		
62	Failure to comply with the requirement to notify a cardholder	Section 33(16)	A fine of not more than N1 million
63	Purchase or sale of cards other than from an issuer or his authorized agent	Section 35	A fine of N500, 000.00 and is also liable to pay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholders.
64	Use of emails, attachments or fraudulent websites to obtain information or details of a cardholder with intent to defraud	Section 36 (1)	Imprisonment for a term of 3 years or to a fine of N1 million or both
65	Fraudulently re-directing funds transfer instructions	Section 36(2)	Imprisonment for a term of 3 years or to a fine of N1 million and is also liable to pay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.
66	Failure to obtain proper identity of customers before executing customers electronic instruction	Section 37(2)	Fine of N5million on conviction
67	thorized debit	Section 37(3)	Fine of N5million on conviction
68	Failure to safely keep data obtained, processed and retrieved for the purpose of law enforcement	Section 38(1-6)	Imprisonment for a term of 3 years or to a fine of N7 million or both

69	Failure by service provider to produce the identity of persons who commit cybercrime, the equipment used etc	Section 39(3)	Fine of not less than N10 million on conviction and an Imprisonment for a term of 3 years or to a fine of N7 million or both for the Director or manager
70	Obstruction and refusal to release information	Section 46	Imprisonment for a term of 2 years or to a fine of N5 million or both

Some Criticisms of the Act

This section examines some critical thoughts about the Act and how it can impact the implementation of the Act and also enforcement of cybercrimes in the Nigerian polity.

Controversy as to the Constitutionality of the Act

As peculiar with virtually all legislations, especially where such legislation tends to create new offences in the jurisprudence of a legal system already flogged with too many legislations bordering on offences, the Cybercrimes (Prohibition, protection, etc) Act, 2015 is one of those Legislations that carefully carved out offences relating to the use of cyberspace. However, it must be observed that legislative powers in Nigeria are drawn from the Constitution of the Federal Republic of Nigeria, 1999 (as amended).[54] The second schedule to the Constitution specifically states in clear terms the Legislative powers of the three arms of government and cybercrime is not listed. There is nowhere in the Act that gives the impression under which of the constitutional provisions the National Assembly promulgated the Act.[55] Especially where section 2 of the Act makes the Act applicable throughout the federation. The difficulty posed

[54] Constitution of the Federal Republic of Nigeria (CFRN), 1999 (as amended), s.4.

[55] F.E. Eboibi, (n.3) at 137-138.

by the Act is that when juxtaposed against the jurisprudence of our legislative system since cybercrime or criminal law is not mentioned in the Exclusive or concurrent legislative list, it ought to be under the legislative confine of the States being a residual matter.[56] Although there is no present judicial interpretation of the legality or otherwise of the Act, solace can arguably be found in the global practice where issues bordering on cyberspace is legislated upon by the National government.[57] Consequently, the Federal Government of Nigeria being the sole manager of our cyberspace could be deemed to have competently enacted the Act to protect cyberspace through the National Assembly. The justification of the Act could arguably be further drawn from item 68 of the exclusive legislative list, which empowers the National Assembly to legislate on matters incidental and supplementary to its powers. It is, however, suggested that the National Assembly, through its incumbent powers, should amend the Constitution. Ensure to reflect this novel issue as falling within the exclusive legislative domain of the National Assembly as the legitimacy of any law, rule, and enactment in the governance of Nigeria is determined by the Nigerian Constitution.[58]

No Specific Mention of Enforcement Institution by the Act

Although the Act made provision for different cybercrime offences, it, however, surprisingly failed to make appropriate provisions as to the manner of enforcement of its provisions. The Act also failed to

---

[56] See the case of *Emelogu v. The State* (1988) NSCC (vol. 19, pt. 1) 869 and the case of *Aminu Tanko v. State* (2009) LPELR-3136 (SC).

[57] See generally F.E Eboibi, (n.3); F.E Eboibi, 'Regulation of Cybercitizen's Conduct on Cyberspace: The Constitutionality and Applicability of the Nigerian Cybercrimes Act 2015' (2018)1(1) *National Journal of Cybersecurity Law*, 37-55.

[58] *Aminu Tanko v. State* (n.56).

state in detail the Law enforcement agencies that should be in charge of the enforcement of the provisions of the Act. Granted that the Act imposed a duty on the ONSA to be in charge of the enforcement of the provisions of the Act, the definition section of the Act defines Law enforcement agencies to include "any agency for the time being responsible for implementation and enforcement of the provisions of the Act."[59] This definition by the Act does not help determine which particular agency should investigate and prosecute the perpetrators of cybercrime in Nigeria. What can be discerned is that any law enforcement agency in Nigeria can as a matter of law investigate and prosecute perpetrators of cybercrime i.e the Nigerian Police Force (NPF), Directorate of Security Services (DSS), Econiomic and Financial Crimes Commission (EFCC), Independent Corrupt Practices Commission (ICPC) etc. The problem here is that most of these agencies do not have the requisite technological skill to investigate cybercrime offences. These offences are very complex due to the nature of electronic transactions that makes the investigation process difficult for forensic and digital investigators to trace, detect, and prevent. Hence, for these agencies to be successful in investigating cybercrime, they must be skilled in the application of forensic data extraction technologies in carrying out an investigation.[60] Moreover, a significant issue is the current lack of synergy amongst law enforcement agencies in Nigeria. There is a distraction, unnecessary interference, and rivalry amongst law enforcement

---

[59] The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.58.

[60] A. Abiodun *et al*. 'Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019) 2(1), *International Journal of Cybersecurity Intelligence & Cybercrime* 56, 63.

agencies, and this inhibits the quality of their investigations, leading to failure in a trial.[61]

The legal implication of the foregoing is that where a particular agency without appropriate forensic and technological know-how charges a cybercrime perpetrator to court. Where he is acquitted for lack of evidence, then, later on, new evidence comes to light due to the diligence of another agency, showing beyond doubt that the perpetrator committed the crime, he cannot be tried a second time. He will have the defence of double jeopardy. Consequently, there should be clarity as to the Law enforcement agencies that are in charge of the enforcement of the provisions of the Act. The Act should be amended to include a specific agency or commission which should be responsible for the investigation of cybercrimes under the Act. Such an agency should be equipped with the required technical skills to enforce the provisions of the Act adequately.

Overlapping Nature of the Act with other Enactments

There are several instances where the Act seems to have overlapped with other enactments of the National Assembly, thereby creating confusion as to which of the enactments should supersede the other. For instance, the Central Bank of Nigeria Act and Banks and Other Financial Institutions Act (BOFIA) had before the enactment of the Nigerian Cybercrimes Act equip the Central Bank of Nigeria with regulatory powers over all financial institutions in Nigeria. However, section 37(3) of the Nigerian Cybercrimes Act by its very nature has overlapped the provisions mentioned above by imposing responsibility on financial

[61] Y. Akinsuyi 'Confusion as the Police and DSS Parades Two Sets of Suspects' *This Day Newspaper* Nigeria, 14 October 2015 at 9.

institutions to reverse within 72 hours any unauthorized debit made on account of a customer. Failure to comply is seen as a cybercrime offence. Arguably, this provision having usurped the express regulatory powers of the CBN contradicts the CBN Act and BOFIA.[62]

Again section 17(4) of the Nigerian Cybercrimes Act contradicts section 93(2) of the Evidence Act 2011. Section 17(4) excludes "creation and execution of wills, codicils and or other testamentary documents, death certificate, birth certificate, matters of family law such as marriage, divorce, adoption or related matters, issuance of court orders, notices, official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments, a cancellation or termination of utility services"[63]… "from the categories of transactions or declaration that are valid by virtue of electronic signature."[64] On the other hand, section 93(2) provides that "Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences."[65] The corollary is that while section 17(4) excludes the use of electronic signature for certain transactions, section 93(2) allows its use with respect to any form of a document. Assuming there is a conflict between the two statutes, which of them supersedes the other, especially where they are enactments of the National Assembly? The case of *Federal Republic of Nigeria v.*

---

62 See Oluwakemi Oluwafunmilayo Oke *et al* 'An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention Etc) Act 2015*'* < http://ssrn.com/abstract> accessed 10 August 2019.

63 The Cybercrimes (Prohibition, Prevention Etc) Act, 2015, s.17(4).

64 *Ibid.*

65 Evidence Act 2011, s. 93(2).

Osahon,[66] gives an insight into the legal implication when it held that where two laws made by the National Assembly conflict, the provisions of the specific enactment will override that which is of general application. However, where the Constitution provides for the situation in conflict, then the Constitution will automatically govern the interpretation. Oluwakemi[67] argues in this regard that since the provisions of both sections 17(4) and 93(2) are specific enactments made by the National Assembly relating to electronic signature, the position of the Court in *Federal Republic of Nigeria v. Osahon*[68] does not apply, especially as the Constitution did not provide for electronic signature. He concluded that it is only the Courts that can resolve this inconsistency in determining which of the Act supersedes the other.

Conclusion

The Cybercrimes (Prohibition, Prevention, etc) Act, 2015 is the first comprehensive legal framework regulating the conduct of internet users in cyberspace. The necessity of the Act and its impact in the fight against cybercrime cannot be overemphasized. This paper has given an analysis of the Act and the intendment of the drafters. However, it raises concerns about some of the provisions of the Act and how these may affect the successful implementation and enforcement of the Act. Suggestions have also been made towards making the Act a workable tool in the quest to curtail the proliferation of cybercrime in Nigeria: The National Assembly should amend the Nigerian Constitution to specifically bring cybercrime under the exclusive legislative list. In the absence of specificity of the appropriate agency that should investigate

---

66 (2006) 5 NWLR (pt 973) 361

67 Oluwakemi *et al supra* 10-11.

68 *Federal Republic of Nigeria v. Osahon* (n.66).

cybercrime in Nigeria, the Act should be amended to provide for a specific agency or Commission. Such an agency or Commission should be equipped with the required technical skills to enforce the provisions of the Act adequately. Moreover, other aspects of the Act that are in conflict with enactments in force should be amended or harmonized with other existing laws. There is a need for the Nigerian government to explore these suggestions.