Journal of Law and Judicial System
Volume 4, Issue 1, 2021, PP 1-11
ISSN 2637-5893
DOI: https://doi.org/10.22259/2637-5893.0401001

Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement

Abayomi B. Sogunle*

LL.B. (Ogun), LL.M. (Lagos), Senior Lecturer and Head, Department of Public Law,Faculty of Law, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria.

***Corresponding Author:** Abayomi B. Sogunle, LL.B. (Ogun), LL.M. (Lagos), Senior Lecturer and Head, Department of Public Law,Faculty of Law,Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria.*

ABSTRACT

In the past decade, there has been an explosion in cybercriminal activity in Nigeria, occasioned by the evolutionary impact of the digital world along with the phenomenal growth and economic power associated with it. The emergence of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 in Nigeria could not have come at a better time, especially in the light of the manifest gross inadequacy of the country's traditional criminal laws which focus their legal objects on physical objects, when as a matter of fact, cybercrimes attack intangible objects, such as information and information technology; and also because cyber-security plays an important role in the ongoing development of information technology as well as internet services which are critical to a country's security and economic wellbeing. The Act having been salutes as an appropriate legislation against the misuse of the information and communication technologies for crimes or other purposes intended to prejudice the integrity of national critical infrastructures, this paper analyses the Nigerian legal framework for combating cybercrimes, the numerous challenges confronting it; and of course, given the virtual and unlimited expansibility nature of cybercrime, the paper concludes with suggestions for a more structured approach to combating the scourge.

Key Words: *Law; Crime; Cybercrime; Economic Crime*

INTRODUCTION

The entire world today has become one global village1. The internet is one of the fastest growing areas of technological infrastructure development and it has penetrated into all fields of social life. This, in turn, has led to the development of the modern concept of the information society.2

This development of the information society offers great opportunities, the most important of which is that unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened in Easter Europe and North Africa).3

However, the development of digital technology and the convergence of computing and communication devices have given rise to a range of opportunities for the use of technology to commit crimes, thus presenting significant challenges to government and law enforcement.

The need to apply new laws and regulations to stem the tide of online criminal activities and also to harvest available internet driven revenue sources when possible for economic benefit has thus become the concern of responsible governments all over the world, and Nigeria is not an exception here. This is so because

[1].*See Michael Litherland and Matt Bross, From Civil to Cyber Rights, A. Perspective on Cyber Policy Challenges in our connected world, available at www.sciencedirect.com, accessed on 3 March, 2021. P. Michael and Anor wrote further on page 2 of their paper as follows: "A typical mobile internet user can carry their personal and direct access into the vast digital world right in their pocket or purse. Advanced communications technologies have connected people, businesses around the globe enabling an individual to quickly reach across vast distances, borders and cultures to engage and interact instantly with someone else."*

[2].*See Yoneji Masuda, The Information Society as Post Industrial Society (World Future Society, Washington, D.C., 1981, 2.*

[3].*See Prof. Dr., Marco Gercke, Understanding Cybercrime Phenomena, Challenges and Legal Response, (September 2012), available at www.itu.int/ITU.D/Cyb/cyber-security/ registration.htm accessed on 3 March, 2021.*

traditional criminal crimes do not have the characteristic of virtuality and unlimited expansibility. Cybercrime, however, represents the growing sophistication of existing criminal behavior and the emergence of novel illegal cyber activities which needs to be faced down and defeated by all responsible governments. Considering the fact that the problem is growing exponentially, the need for legal acts combining law and technology has become imminent. The cybercrimes (Prohibition, Prevention, etc.) Act of 2015, therefore, underscores the fact that the internet needs to be governed by laws and that norms must be developed so as to ensure a certain degree of central control.

Incidentally, issues bordering on criminal abuse of information technology and the necessary legal response have dominated legal discourse ever since the technology was introduced. Various solutions have been implemented in many advanced countries. In spite of this, the issue of cybercrime has remained a very challenging one on account of constant technical development as well as changing methods and ways in which the offences are committed.

The problem of cybercrime has, thus, engaged the attention of the United Nations and other international organizations. While in the beginning the United Nation's response was limited to general guidelines4, the Organisation has in recent times dealt more extensively with the challenges and legal response5.

In March 2010, the UN General Assembly passed a new resolution6 as part of the "creation of a global culture of cyber security" initiative. The particular resolution refers to the two major resolutions on cybercrime7. The voluntary self-assessment tool for national efforts to protect critical information infrastructure provided as an annex to the resolution calls for countries to review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of, and dependence upon, new information and communication technologies. The resolution further calls on states to use regional international conventions, arrangements and precedents in their reviews8. In Nigeria, clear evidence of attacks against information systems abound, in particular as a result from organized crime, and increasing concern at the potential of Boko Haram attacks against information systems which form part of the critical infrastructure of Nigeria. This, no doubt, constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice. Nigerian government, therefore, in realization of the urgent need for legal acts combining law and technology in line with the March 2010 UN. General Assembly Resolution as a veritably instrument for combating the scourge of cybercrime, came up with the Cybercrime (Prohibition, Prevention etc.) Act, 2015.

The Act is divided into Eight (8) different parts. Part 1 spells out the objectives and applications of the Act; Part II deals with protection of critical National Information Infrastructure; Part III centers on offences and penalties; Part IV contains Duties of Financial Institutions; Part V relates to Administration and Enforcement; Part VI captives Arrest, Search, seizure and

---

4. *See United Nations Convention on the Rights of the Child, adopted in 1989 (A/RES/44/25) which contains instruments aiming to protect children. It does not define child pornography, nor does it contain provisions that harmonise the criminalization of the distribution of online pornography. However, Art. 34 calls upon. Member states to prevent the exploitative use of children in pornography performances. See also the United Nations General Assembly Resolution No. 45/121 (1990) containing a UN. Manual on prevention and control of computer related crime. (United Nations Publication, Sales No. E 94. IV. 5)*
5. *See Resolution 55/63 adopted by the U.N. General Assembly in Vienna in 2000. In its resolution, the General Assembly in Vienna in 2000 identified a number of measures to prevent the misuse of information technology, including the fact that states should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technology etc., see also Resolution 56/121 of the UN General Assembly of 2002 which underlines the need for cooperation among states in combating criminal misuse of information technology.*
6. *Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure A/RES/ 64/211.*
7. *Resolution 55/63; 56/121.*
8. *Prof. Dr. Marco Garcke, Understanding Cybercrime: Phenomena, Challenges and Legal response (September 2012), available online at www.itu.int/ITU_D/cyb/cybersecurity/legislation .html,119 accessed on 3 March, 2021.*

Prosecution; Part VII captures issues relating to Jurisdiction and International Cooperation and Part VIII deals with miscellaneous matters.

Part I which relates to objectives and application declares the objectives of the Act to follows:

- To provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
- To ensure the protection of critical national information infrastructure; and
- To promote cyber security and the protection of computer, systems and networks, electronic communications, data and computer program, intellectual property and privacy rights9.

From the general reading of the Act, it is clear that the Act fails to provide the definition of the term "cybercrime" which incidentally is the subject matter of the legislation itself.. This, it is submitted, is not unconnected with the inconsistencies in the cybercrime vocabulary engendered by the lack of a unanimous perception that would sufficiently represent cybercrime as an umbrella term for the technology induced types of offences10. For instance, D. Wall defines cybercrime thus:

Cybercrimes are criminal or harmful activities that are informational, global and networked and are to be distinguished" from crimes that simple use computers. They are the product of networked technologies that have transformed the division of criminal labour to provide entirely new opportunities and new forms of crime which typically involve the acquisition or manipulation of information and its values across global networks for gain. They can be broken down into crimes that are related to the integrity of the system, crimes in which networked computers are used to assist in perpetration of crime, and crimes which relate to the content of computers11

As broad as this definition is, the difficulty with the definition is that it would not cover traditional crimes such as murder and some other offences. For example, an offender using a keyboard to hit and kill a victim is not covered here. Those cases where physical hardware is used to commit regular 1crime are excluded12.

However, the Stanford Draft International Convention to Enhance Protection from Cybercrime and Terrorism defines cybercrime to mean "conduct, with respect to cyber systems that is classified as an offence punishable by the Act"13. This definition, no doubt, would include

---

9. *Section 1, Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.*
10. *Erika Kraemar-Mbula, Puay Tang & Howard Rush, in The Cybercrime Ecosystem: Online Innovation in the Shadows, Technological Forecasting and Social Change, 80 (2013) 541-553, have this to say on cybercrime definition: "Cybercrime takes many forms, depending on its final purpose and means and classifications are as varied as the number of studies on the subject" at 543; Duygu Solak and Murat Topaloglu in The Perception Analysis of Cybercrimes in View of Computer Science Students, Procedia, Social and Behavioural Sciences 182 (2015) 590-595, define cybercrime thus: "Cybercrime is any kind of illegal, unethical and unauthorized behavior in a system which processes information automatically or transfer data" at 591; Ajayi, E F. G, in Challenges to Enforcement of Cybercrimes Laws and Policy, Journal of Internet and Information System, Vol. 6 (1) August 2016; 1-12, lamenting on this dilemma said: "Due to dichotomies in Jurisdictions and yet addressing the same concept in legal literature, cybercrimes to date has no globally accepted definition that could possibly encapsulate all the facets of this novel brand of crime, the definitional problem of cybercrime subsists, but one thing that is certain is that most definitions of cybercrime make reference to the internet…. For the sake (of) overcoming the lacuna, cybercrime has been defined as crime committed over the internet which might include hacking, defamation, copyright infringement and fraud. According to Oxford Dictionary of Law (2002), Cybercrime also means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of the" at p. 2*
11. *D. Wall, Cybercrime: The Transformation of Crime in the Information Age, Policy Press, Cambridge, 2007.*
12. *See also Chang E, Chung W, Chan H., Chou S., (2003), An International Perspective on Fighting Cybercrime, ISI' 03 Proceeding of the 1st NSF / NIJ Conference on Intelligence and Security Informatics, pp. 379-384 where cybercrime is defined as "illegal internet-mediated activities that often take place in global electronic network"*
13. *Article 1: 1 Draft International Convention to Enhance Protection from Cybercrime and Terrorism,1999, available at http://media.*

cases where physical hardware is used to commit regular crime.

Considering the fact that there is no simple definition of cybercrime, the draftsmen of the Act adopted the approach found in the Convention on Cybercrime14 which distinguishes between four different types of offences15 namely: offences against the confidentiality, integrity and availability of computer data and system16; computer related offences17; content related offences18 and copyright related offences19 (this last one is not captured in the Act).

Suffice it to say however that this typology is not wholly consistent as it is not based on a sole criterion to differentiate between categories. Thus first three categories focus on the object of legal protection, offences against confidentiality, integrity and availability of computer data and systems, content relate offences and copyright related offences.

Offences against Confidentiality, Integrity and Availability of Computer Data and Systems

Reliance on digital technology, particularly networked communication, is now so pervasive that it is regarded as part of the critical infrastructure. The volume of sensitive government and commercial information stored and transmitted electronically raises the potential for espionage20.

Under the Act21, offences included in this category are unlawful access to a computer22; unlawful interceptions23 and system interference24. Of course, given the ubiquitous presence of computers in modern life and the dependency of modern commerce on computer networks, such offences have potentially serious consequences.

Unlawful access to a computer is analogous to illegal access to a building and is recognized as a criminal offence under the Act25. Illegal access to computer systems hinders computers operators in managing, operating and controlling their systems in an undisturbed and uninhibited manner. The aim of course is the maintenance of the integrity of computer systems. However, the question that may arise here has to do with whether unlawful access is the end goal here or the unlawful access envisaged by the provisions of section 6 extends to further crimes committed after the initial access such as modifying or obtaining stored data (where law seeks to protect integrity and confidentiality of the data)26. In other words, does the Act criminalize the act of illegal access in addition to subsequent offences? This question is relevant because enacted provisions sometimes confuse illegal access with subsequent offences. However, it is submitted here that a conjunctive reading of the provisions of section 6 of the Act shows that the provisions criminalize both illegal access and subsequent offence. Section 6 (i) talks about the issue of access "in whole or in part". Furthermore, section 6 (2) goes on to provide a stiffer penalty where the illegal access indicated in subsection 1 is committed with the intent of obtaining computer data etc. Also, the section requires that

hoover.org/documents/0817999825. 221.pdf accessed on 3 March, 2021.

14. *Council of Europe Convention on Cybercrime (CETS No. 185) available at: http://conventions. co.int. accessed on 3 March, 2021.*
15. *Report available at: www.itu/osg/csd/ cyber security/gca/globalstrategicreport/index.html accessed on 3 March, 2021.*
16. *Art 2. (Illegal access) Art 3 (Illegal interception) Art 4 (Data Interference), Art 5 (System Interference Section 8 or the Act), Art 6 (Misuse of Device Section 36 of the pet).*
17. *Act 7 (Computer Related Forgery Section 13 of the Act), Art 8 (Computer related fraud Section 14 of the Act.*
18. *Art 9 (Offences related to child pornography) Section 23 of the Act.*
19. *Art 10 (Offences related to infringement of copyright and related rights)*
20. *Jonathan Clough, "Cybercrime", Commonwealth Law Bulletin (2011) 37:4 671-680, at 675.*
21. *Cybercrimes (Prohibition, Prevention etc) Act, 2015.*
22. *Section 6 of the Act.*
23. *Section 12 of the Act.*
24. *Section 8 of the Act.*
25. *Section 6 (i) provides in part: "Any person, who, without authorization, intentionally accesses, in whole or in part, a computer system or network for fraudulent purpose and obtain data that are vital to national security, commits an offence….." Section 6 (2) says: "where the offence provided un subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program commercial or industrial secrets or classified information……"*
26. *See Prof. Dr. Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal response, (September 2012), available online at www.itu.int/ITU-D/Cybersecurity/legislation/html.page accessed on 3 March, 2021, 179.*

the act of unlawful access must have been committed with the requisite intention.

Another element of the offence created by section 6 of the Act is that the "access to a computer" can only the committed if it takes place without authorization. In the light of this, it is submitted that the section explicitly aims to incorporate the concept of self defence.

However, the provisions of section 6 can run into difficulties where a computer system was not accessed unlawfully, but the user continues to use the system after permission had expired.

It is therefore, suggested that a provision similar to section 5 of the "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedure Cybercrime Legislative text"27 be included in the Act to clear doubts in this regard. Section 5 of the Enhancing Competitiveness in the Caribbean ICT Policies, Legislation Regulation Procedure provides: Illegal Remaining A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable in conviction, by imprisonment for a period of not exceeding (period), or a fine not exceeding (amount) or both. Unlawful interception28

Section 12 of the Act underscores the importance of computer data to private users, businesses and administrators. Lack of data can cause considerable damage in terms of finance to users.

A careful reading of the section shows that its applicability is limited to the interception of data by technical means. Also, the section talks about interception of "non-public transmissions". First it must be realized the "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer. A transmission is "non-public" if the transmission process is confidential29. According to Gercke30,the "vital element to differentiate between public and non-public transmission is not the nature of the data transmitted but the nature of the transmission process. Even the transfer of publicly available information can be considered criminal, if the parties involved in the transfer intend to keep the content of their communication secrete"

SYSTEM INTERFERENCE

The Act also criminalizes the intentional hindering of lawful use of computer system31.

---

27. *Enhancing Competitiveness in the Caribbean Through ICT Policies, Legislation and Regulatory Procedure 1980, available at www.itu.int/ITU-D/projects/ITU EC ACP/icb4pis/index.html accessed on 3 March, 2021.*

28. *Section 12 (i) of the Act "Any person who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a five of not more that ₦5,000,000:00 or to both such fine and imprisonment. Cf with Article 3 of the European Convention on Cybercrime, 2000, which provides: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system." (CETS No. 185) available at: http://conventions.co.int accessed on 3 March, 2021.*

29. *Prof. Dr. Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, (September 2012), available on www.itu.int/ITU-D/cyb/cybersecurity/legislation.htmlat accessed on 3 March, 2021, 186.*

30. *Ibid, at 186.*

31. *Section 8 of the Act provides "Any person who, without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating; altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 to both fine and imprisonment. Contrast with Art 5. Of the European Convention on Cybercrime, 2000 and section 7*

No doubt, the application of this section is limited to cases where hindering is "serious" and is carried out by ones of the acts mentioned thereunder. Also the offender must be carrying out the offences "intentionally" or for fraudulent purposes and the act must have been done without lawful authority. Also criminalized are acts that render computer data inaccessible.

However, the requirements that the particular section can be invoked only where the hindering is a serious one is likely to cause confusion as legal arguments here may center on the criteria to be fulfilled for determining whether the hindering of the functioning of the computer system is serious or not. To obviate unnecessary arguments here, it is submitted that a provision similar to section 7 of the 1999 Stanford Draft International Convention be adopted to replace section 8 of the Nigerian law. The section in question provides[32].

"7 (1) A person who intentionally or recklessly without lawful excuse or justification:

(a) hinders or interferes with the functions of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction for a period not exceeding (period), or a fine not exceeding (amount) or both in subsection (i) "hinder," in relation to a computer system, includes but is not limit to:

(a) cutting the electricity supply to a computer system, and

(b) causing electromagnetic interference to a computer system by any means; and

(c) corrupting a computer system by any means; and

(d) inputting deleting or altering computer data"

The incorporation of the definition of the word "hinder" in the above section in our section 8 is necessary to widen the list of the acts by which the functioning of a computer system may be affected adversely.

Content Related Offences

The content related offences captured under the Act include child pornography and related offences[33], and racist and xenophobia offences[34].

Child Pornography

Child pornography offences have a harmful repercussion in society and specifically for minor victims as a vulnerable sector in these matters[35]. No doubt the provisions of section 23 are in line with international best practice as offences in this regard are universally recognized as criminal acts[36]. The offence here can only be committed with requisite intention. This section seeks to modernize child pornography laws and to attach consequences to the conduct of each participant in the chain,

of the 2002 Commonwealth Model Law, available at www.thecommonwealth.org/shared asp files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77=86970A639805%7 Computer%20Crime.pdf (Annex1). The latter also criminalizes "reckless" acts accessed on 3 March, 2021..

[32]. *Section 7 of the 1999 Stanford Draft International Convention available at http:// media,hoover.org/documents/0871999825 249.pdf. accessed on 3 March, 2021.*

[33]. *Section 23 of the Act.*

." It provides in part: Any person who intentionally uses any computer system or networking in or for:-

(a) Producing child pornography; (b) offering or making available child pornography (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person. (e) possessing child pornography in a computer system or on a computer data storage medium: commits an offence under the Act and…."

[34]. *Section 26 of the Act. It provides in part: "Any person who with intent – (a) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network; (b) threatens through a computer system or network – (i) persons for the reasons that they belong to a group distinguished by race, colour, descent, national or ethnic origin….."*

[35] *Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime(UNDO), (February 2013)*

[36]. *See 1989 United Nations Conventions on the Rights of the Child, available at www.g8.gc.ca/genoa/july-22-01-1-e.asp accessed on 3 March, 2021; 2003 European Union Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography; available at: http://eur-;ex.europe.en/Lexuriserv/site/en/oj/2004/1013/ 101320040120en004400e8.pdf, accessed on 3 March, 2021 and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, available at: http://conventions.coe.int.*

creating offences of production, offering/making available, distributing/ transmitting, procuring and possessing.

However, the challenges here have to do with the fact that countries may differ on the appropriate age of consent, whether 'simple' possession should be criminalized and whether the definition of child pornography should include 'materials that visually depicts' as contained in our Section 23, or not

Another problem associated with the enforcement of section 23 is succinctly captured by Prof. Marcon Gercke when he observes thus37:

"The legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world. If offenders create content that is illegal in some countries, but not in the country they are operating from, prosecution of the offenders is difficult or impossible. There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized"

Analogous to the above position is the vexed issue of how to enforce section 23 without interfering with the right to freedom of expression38.

Racist and Xenophobic Offences

From the clear provision of section 26 of the Act, intentional distribution and making available of xenophobic material to the public through a computer system is an offence.

One of the shortcomings of the Nigeria Act is that it does not define what constitutes a "racist and xenophobic material". However, it is deducible from the wordings of section 26 that a racist and xenophobic material will include any material which advocates, promotes or incites hatred, discrimination or violence against persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors; or a group of persons which is distinguished by any of these characteristics39" Insulting public through a computer system or network persons captured in the preceding sentence is also an offence40.

It is submitted here that the word "threatens" in section 26 (1) (b) does not require any interaction with the public as the Act only criminalizes threats made "through a computer or computer network"

Also section 26 (i) (c) criminalizes insults made "publicly through a computer system or network to persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors" This particular provision obviously excludes insults made through private communication e.g. e-mail as that would not qualify as insult made publicly.

However, the Act fails to define what constitutes "insult." If the word "insults" is understood to refer to any offensive or invective expression which prejudices the dignity of a person and is directly connected with the insulted person's belonging to the group, then there is the need for caution here to ensure that the sanctity of the principles of freedom of speech as guaranteed under the constitution41 is not violated. Obviously, in order to safeguard the principles of freedom of expression guaranteed under the constitution, there would be the need for the court to interpret the act of insult envisaged under section 26 of the Act narrowly.

Computer-related Offences

Computer related offences suggest offences where the computer is used to facilitate the commission of an offence. Included in this category under the Act are Computer related forgery42, computer related fraud43 and identity theft and impersonation44.

Computer-related Forgery[45]

[37]. *Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, (September 2012), available at: www.itu. int/ ITU-D/Cyb/cybersecurity/legislation.htmlatpage21, accessed on 3 March, 2021.*

[38]. *Section 39(1) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).*

[39]. *Section 26 (1)(b) (i) of the Act.*

[40]. *Section 26 (1) (c) (i) of the Act.*

[41]. *Section 39(1) Constitution of the Federal Republic of Nigeria 1999 (as amended) ibid (n 38).*

[42]. *Section 13 of the Act*

[43]. *Section 14 of the Act*

[44]. *Section 22 of the Act.*

[45]. *Section 13 of the Act provides "A person who knowingly accesses any computer or network*

From the clear reading of section 13 of the Act, computer related forgery seeks to protect data. Clearly the provision does not only refer to computer data as the object of one of the acts mentioned, it is also necessary that the acts result in inauthentic data.

Computer-related Fraud[46]

Fraud is one of the most common forms of cybercrime. Examples include fraudulent online sales, advance fee schemes (otherwise known as 419), fraudulent investment opportunities and fraudulent electronic transfer of funds. Section 40 of the Act criminalizes an undue manipulation in the course of data processing with the intent to effect an illegal transfer of property. However, for offences listed under section 14 (1) - (5) of the Act, the offender must have acted "intentionally". The intent here has to do with the "manipulation" as well as the "financial loss."

Identify Theft and Impersonation

Identify theft and impersonation refers to the criminal act of fraudulently obtaining and using another person's identity. The inclusion of Section 22 in the Act is commendable. It is a recognition of the fact that while criminal law has traditionally focused on the use of false identities in the commission of crime, there had been a gap in the law to punish the preliminary steps of collecting, processing and trafficking identity information. It contains three different phases. According to Marco Gercke47 "the first phase the offender obtains identity related information. This part of the offence can for example be carried out by using malicious software or phishing attacks. The second phase is characterized by interaction with identity related information prior to the use of the information within criminal offences. The third phase is the use of the identity related information in relation with a criminal offences. In most cases, the access to identity related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities"

It is submitted that Section 22 of the Act covers a wide range of offences related to identity theft within the ambit of the 3 phases identified by Marco Gercke above, as criminalization within the provisions of section 22 is not limited to any given phase.

Jurisdiction[48]

The criminal jurisdiction of computer cybercrime is different from the traditional crime. The typical one is "abstract cross border" behavior. Since the criminal act involves many countries, it is difficult for this illegal computer cybercrime to point to a certain area of criminal jurisdiction. This issue of abstract "cross border has formed a great challenge to the traditional theory of criminal jurisdiction of computer cybercrime.49 This explains the provisions of section 50 of the Act. Section 50 provides in part:

50 (1) The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to dry offences under this Act, if committed -in Nigeria or in a ship or aircraft registered in Nigeria; or by a citizen or resident in Nigeria if the persons conduct would also constitute an offence under a law of the country where the offence was committed; or outside Nigeria, where -the victims of the offence is a citizen or resident in Nigeria; or the alleged offender is in Nigeria and not extradited to any other country for presentation……

and inputs, alters, delete, or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible comits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less that ₦7,000,000 or both".

46. *Section 14 of the Act. "Section 14 (1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring economic benefits on himself or another person, commits an offence and shall be liable on conviction to imprisonment for a term not less than 3 years, or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonments"*

47. *Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response available online at www.itu.int/ITU-D/Cyb/Cybersecurity/legislation.html, accessed on 3 March, 2021, 32.*

48. *See Section 50 of the Act.*

49. *This usually results in conflict of jurisdiction, detrimental to the trial of the facts of the case and protection of the legitimate rights and interest of the victims.*

From the reading of section 5050, there is no iota of doubt that section 50 (1) (a) (b) and (c) is a codification of the principle of territoriality51. The fact that jurisdiction in general only makes sense if it can be enforced, and enforcement of law requires control explains the relevance of the principle in computer cybercrime matters.

However, the problem with section 50 (1) (a) - (c) has to do with a situation where neither the offender nor victim is located within the country but only the infrastructure within a country was used for the commission of a crime. For example, if an e-mail with illegal content was sent out by using an e-mail provider in another country or a website with illegal content is stored on the server of a hosting provider to the country?

To deal with a problem such as this, it is suggested that a provision similar to the Singapore Act52 be included in the Nigerian cybercrime Act.

Challenges to Enforcement

It will be appreciated that cybercrime is in a class of its own. It is unique and distinct in character, unlike the traditional terrestrial crimes which are committed in a particular locus and whereof, the effects are felt by the victims. In other words, cybercrimes are cross border or transnational crimes.

In the light of the above, one major challenge to the enforcement of the Nigerian Act is jurisdiction. Although section 50 of the Act seeks to provide a solution in this respect, the issue is not as simple as it appears.

Under section 50 (1) (c) of the Act, Nigeria retains jurisdiction to conduct trials over her nationals or resident for offences committed abroad provided that the act in question constitutes an offence under the law of the country where the offence was committed. This is known as the dual criminality principle.

The nagging question here is what happens when the Nigerian citizen's/resident's conduct constitutes an offence under the cybercrime Act of 2015 but it is not so under the foreign law? The requirement of section 50 (i) (c) of the Act presents an insurmountable challenge to the enforcement of the Act53.

Absence of Capacity Building

The profuse use of internet is increasingly globalizing. In other words, cybercrime is a global issue. The growth of the required skills to perpetrate cybercrime and the spread of broadband infrastructure are driving the fast global redistribution of the geographical locations of cybercrime. Cybercriminals are experts in computer and cyberspace issues, thus, the expertise of cybercrime cannot be compared with Nigerian enforcement agencies who are merely government officials without the requisite skills. They are ill-trained, poorly remunerated and more often than not, offer

---

[50]. *Article 22 of the European Convention on Computer Cybercrime, 2001 provides: Each party shall adopt such legislationss and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Article 2 through 11 of this convention, when the offence is committed:*

(a) In its territory; or

(b) On board a ship flying the flag of that party; or

(c) On board an aircraft registered under the laws of that party; or

(d) By one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state.

[51]. *It is applicable if the offence – regardless of the nationality of the offender or victim- is committed within the territory of a sovereign state.*

[52]. *See Section 11 (3) (b) Singapore Computer Misuse Act, 2007*

11 (1) Subject to subsection (2), the provision of this Act shall have effect in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any Person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act shall apply if, for the offence in question –
(a) the accused was in Singapore at the material time; or the computer, program or data was in Singapore at the material time.

[53]. *Aside this, fear of inhuman treatment is also a bar to extradition and this basically includes torture, and degrading punishment which are likely to be meted out to the defendant. See Soering V. The United Kingdom (1989) European Court of Human Rights; Extraterritorial responsibility under Article 3 EHRC establishes a legal barrier on deportation or extradition if there are substantial grounds for believing that there is a real risk of treatment contrary to Article 3; Othman (Abu Qatada) v. United Kingdom 81 39/09 (2012) ECHR 56.*

their services without proper security and protection. In this jet age, this is a major drawback. There is therefore a strong need for qualified personnel with adequate knowledge is gathering evidence.

Information and Communication Technology is complex and frequently unfamiliar to the traditional criminal justice system54 to which we are all accustomed in Nigeria. Dealing with crimes involving these devices requires well trained personnel in the investigation phase, during prosecution and in courts. Nigeria cannot boast of this. Consequently, there is the urgent need for capacity building in this regard.

Another challenge besetting the enforcement of the Act is the existence of a multitude of national and international legal frameworks. The legal systems in each level envisage different provisions to measure cybercrime and this can cause legal gaps which make immunity possible on the basis of territoriality55. A critical look at the cyber-content crimes contained under the Act will bring the point being made here clearly. For example, section 23 of the Act deals with child pornography, no doubt. However, the point is, pornography is measured in several different ways some states allow production and distribution of all kinds of pornography, others prohibit pornography using children and some others prohibit all kind of production and distribution of pornography. These different laws offer differentiated treatment for the same conduct. This situation depends on the characteristics and values of each country. Since effective cybercrime legislation is a function of collaboration among countries, this disparity in law could hinder the effective operation of the cybercrime Act of 2015.

Electronic Evidence

Unraveling cybercrime incidents are a function of electronic evidence. Dealing with evidence like this throws up a number of challenges especially in the light of the fact that cybercrime investigation process have to be developed inside of cyberspace where evidence can disappear or be changed in few seconds. In most cases, therefore, ability to successfully identify and prosecute an offender depends identify depends upon a correct collection and evaluation of electronic evidence. This is a big challenge in Nigeria.

Conclusion

No matter how effective a country's local laws, the global nature of cybercrime means that international cooperation is inevitable. Concerted efforts by national and international law enforcement, separately and together, and stringent corporate information security measures are necessary. This may be in order to secure evidence of offending, or to secure the offenders themselves. However, conflict between the competent jurisdictions is a major problem in the global efforts towards stemming the scourge. Existing side by side with this are the absence of a uniform definition of cybercrime, the difficulties relating to gathering and using evidence, detecting cybercrime acts, among others. Also, as laudable as the provisions of the Act are, the near absolute reliance on punishment as the only means of preventing computer cybercrime is serious drawback, and there is the urgent need for the Nigerian government to address this. Over the years it has been proven that prevention is a key component in an effective fight against cybercrime. Measures in this regard can range from technical solutions (such as fireworks that prevent illegal access to a computer system and antivirus software that can hinder the installation of malicious software) to the blocking of access to illegal content.

The point being made here is expressed clearly in the Pacific Island Draft Model Policy for cybercrime56 in the following words:"In addition to the criminalization of cybercrime and the improvement of the ability of law enforcement to combat cybercrime, crime preventions measures need to be developed within the process of developing such measures, that can range from technical solutions to increasing user awareness, it is important to identify those groups that require specific attention such as youth, technologically challenged people (such as people from isolated villages that are technologically unaware) and women.

However, crime prevention measures should also apply to more advanced users and technology - affiliate players such as critical

54. *Jose Grabiel Cordova and Others, Law Versus Cybercrime (Global Jurist, 2018), 4.*
55. *Ibid, 4.*
56. *The approved documents related to the projects are available at www.itu/ITU-D/projects/ITU EC ACP/icbAPis/index.html, accessed on 3 March, 2021.*

infrastructure provider (such as tourism or financial sector). The debate about necessary measures should include the whole range of instruments such as awareness raising, making available and promoting free of charge protection technology (such as antivirus software) and the implementation of solutions to enable parents to restrict the access to certain content.

Such measures should ideally be available at the time of an introduction of a service/technology and maintained throughout its operation. To ensure a wider reach of such measure, a broad range of stakeholders should be involved that range from internet service provider to governments and regional bodies and explore various sources of funding."

Citation: *Olusesan Oliyide," Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement", Journal of Law and Judicial System, 4(1), 2021, pp.1-11. DOI: https: //doi.org / 10.22259 /2637-5893.0401001*