Journal of International Studies Vol. 15, 117-132 (2019)

How to cite this article:

Abdulkadir, A. B., & Abdulkadir, A. 0. (2019). Cybercrimes act in Nigeria: Experimenting compliance with internationally recognized human rights provisions. *Journal of International Studies*, *15*,117-132. https://doi.org/10.32890/jis2019.15.8

Cybercrimes Act in Nigeria: Experimenting Compliance with Internationally Recognized Human Rights Provisions

[1]Abdulkadir Bolaji Abdulkadir & [2]Abdulrazaq Owolabi Abdulkadir
[1&2]Faculty of Law, University of Ilorin, Nigeria
[1]Corresponding author: abdulkadir.@unilorin.edu.ng

DOI: https://doi.org/10.32890/jis2019.15.8

Received: 1/11/2019 Revised: 22/12/2019 Accepted: 23/12/2019 Published: 31/12/2019

Abstract

The occurrence of criminal activities has increased owing to the advent of internet or computer technology. Access to internet has posed serious challenges to the existing legal regime and enforcement paradigm. The recent experience concerning rate of technology and online communication has no doubt fashioned-out a dramatic increase in the incidence of criminal activities. It has also resulted in the occurrence of what is considered as a new approach of criminal activities. Although, the emergence of electronic communication advances economic prosperity of the world's commerce, fraudsters have gained access and seen the medium as a fertile ground for pretence. This paper firstly discusses the wide-ranging descriptions that led to the complex concept of cybercrime. The paper then examines the importance of cybercrimes regulations to curb infidelity in the use of computer technology. It also investigates the interface between cybercrimes and human rights and argued that human rights are an onerous matter that should be given proper consideration when dealing with cybercrime offenders. The paper utilizes legal research method by way of examining the Nigerian Cybercrimes Act 2015 and its relationship with several human rights provisions. It concludes by revealing the need to prevent cybercrimes that coincide with the right of an individual to enjoy his right to privacy and at the same time ensuring cyber security.

Keywords: *Cybercrimes, human rights, compliance.*

Introduction

The advancement of the internet and indeed the unhindered access to computer technology has undoubtedly fashioned new hopes for work and business opportunities. It is also

considered as finicky adventure, especially for those who believed in illicit dealings. The constant increase of technology and communication online or via internet has not only fashioned-out a dramatic development in the incidence of criminal activities, but it also brought a new variety of criminal activities. Both the rise in the occurrence of criminal activities and the probable occurrence of new dimensions of criminal activity presents challenges for legal systems and for the law enforcement agents. Certainly, technology has incorporated nations, thereby making the world to be a global village concern. The major economic advantage of most nations of the world is that, they can be accessed with the aid of the internet connection. Considering its characteristic, the electronic market is available to everybody, pretence and falsehood had its way and finds a fertile ground in this situation. Despite the pretence and falsehood that bedeviled the internet technology, its emergence has given rise to two edge functions: namely that, it engendered progressive values to the world on one hand and produced numerous maladies that threaten the good order of the world on the other hand and also producing a new wave of crime to the world.

The coming of digital technology brought about modern communication internet service, hard-wares and powerful computer systems to access data. Therefore, cyberspace is now seeing as a safe haven for internet platform, that has fashioned geometric growth and increased windows of opportunities for business adventures. It also removes economic barriers initially faced by nations of the world. People of different background and from diverse areas of human endeavour have now been opportune to freely access and utilize the advantages offered by internet platform. However, the emergence of information technology in Nigeria has introduced a new wave of crime. Experience has shown (through proceedings or trial of suspects in Nigerian courts) that a very few minded youth who are criminally, mostly uneducated, drop-out, are stealing and committing crime with the aid of the internet and fictitious online business transactions. The internet technology which ought to be a blessing (considering the fact that it exposes one opportunities in various field) has become worrisome due to the heinous atrocities that represent the order of the day among youth.

It is beyond peradventure that nations have adopted different approaches to battle with crimes depending on their character and indeed extent. A nation with high rate of crime will find it extremely difficult to attain speedy growth or development. In Nigeria situation, (being a country on the threshold of protecting her name on issue of cybercrimes), strenuous efforts are presently being geared towards eradicating channels through which cybercrimes are being perpetrated. It is thus a commendable effort that led to the passing of Cybercrimes Act in 2015. It is on this premise that this paper examines Cybercrimes Act and the extent of its compliance with protected human rights. This is for the obvious reason that the issue of human rights protection cannot be ignored in attempt to guide against crimes and ensure security in a nation. Therefore, the paper is divided into six parts. The first part is introduction, which gives a background study of the paper. The second part examines the concept of cybercrimes with a view to understand what it entails. The third part examines cybercrimes in Nigeria in order to justify the imperative needs to curb such crimes. The fourth part discusses the link between cyber security and the indeed protection of human

rights. This paper argued that the issue of human rights must be put into consideration in an attempt to curb cybercrimes and ensure cyber security. The fifth part explores some major offences in the Cybercrimes Act and the extent of their compliance with protected human rights. The paper argued that the offences provided for under the Cybercrimes Act are designed to protect some specific human rights of individuals. This paper utilizes legal research method by way of analyzing the Nigerian Cybercrimes Act 2015 with several human rights provisions available in national and international regulations.

The Concept of Cybercrime

Identified problem for experimenting cybercrime is the deficiency of a consistent and or statutory definition of activities which may constitute cybercrime. The issue of conceptualizing cybercrime appears intangible complexities. This is because, wide-ranging descriptions of cybercrime do exist. The term is also identified by array of names such as computer-related crime, information technology crime, computer crime, electronic crime and Internet crime.

It has been argued that cybercrime is ancient. Hence, the advent of information technology and unprecedented interconnectivity provided has been a benefit to criminals (A Summary of the Legislation on Cybercrime in Nigeria, December, 2018).

However, it is not within the scope of this paper to go into the jurisprudential debates of cybercrimes instead, the imperative of this part is to provide background knowledge of the concept. Therefore, if cybercrimes is synonymous with the forgoing concepts, a description of any of the concept will be the same as defining cybercrime. Essentially, crimes connected with Computer are as vulnerable, in contradistinction to common physical crimes. The nature of crimes that are currently being perpetrated in the internet have happened before existence of the internet itself. But the dimension appears to have changed.

Thus, various approaches by scholars have been made in recent decades to encapsulate a precise definition for both terms. This paper describes cybercrime in accordance with the Florida Cyber-Security Manual, 2004, has as a planned act, with aid or use of computers and or other technologies, and that illicit activity have to take place in a practical setting, such as the Internet.

Importantly, during the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, efforts were made at offering two definitions within a related workshop. Cybercrime was perceived in a narrow sense and in a broad sense. In narrow perspective, cybercrime includes any unlawful behaviour directed or through the use of electronic operations that has the security of computer systems as the data processed by them as target (Crimes related to computer networks, 2000). Cybercrime in a broader sense on the hand, traverses any illegal behaviour perpetrated by means or in relation to use of a

computer system, network. This includes crimes like illegal possession and disseminating information by means of a computer system or network (Carter, 1995: Charney, 1994). Some definitions attempt to take *mensrea* in to account and this is what informed defining cybercrime as "computer-mediated activities which are either *illegal or considered illicit* by certain parties that can be conducted *through global electronic networks "*(Hale, 2002 p.92*)*. It has been argued that machine automation and data are the hallmark of industrial revolution (Dharfizi, 2018). These more advanced characterizations exclude instances where physical hardware is applied to commit regular crimes. Some have defined cybercrimes according to classification. For instance, in the Council of Europe's Convention on Cybercrime (2001), cybercrimes have been classified into 4 different classifications:

i. Offences relating to the confidentiality, integrity and availability of computer data and systems;
ii. Computer- related offences,
iii. Content related offences; and
iv. Offences related to infringements of copyright and related rights.

Consequently, the range of approaches and the related problems, shows that there are sizeable tasks at defining the term cybercrime. Cybercrime is adopted to describe a series of offences as well as traditional computer crimes and network crimes. The mere fact that there is no consensus definition of the term cybercrime does not mean that such concept is not in existence. This is even more so that what constitute crimes differ from jurisdiction to jurisdiction. Therefore, the description of the term cybercrime depends on the adoption of either a narrow or broad definition. In case a narrow definition is adopted, the meaning of cybercrime will be limited to offences committed via computer with the use of internet. However, a broad definition of cybercrimes will include other computer-related offences without necessarily involving the use of internet. Therefore, this study adopts the later definition, as it embraces offences relating to the use of the internet and computer.

Cybercrimes in Nigeria

Cybercrimes in Nigeria are being carried out by persons, regardless of age, as it varies from young to old, but in most cases, the young. Numerous youth involve in cybercrime with the objective of emerging as the greatest billionaire, or as a profit making scheme since the technologies for hacking in our contemporary world has become affordable by many. It is not surprising that crimes like phishing, privacy intrusion, mail scams, identity theft among others are on the increase in the country (Oyenike, Adebiyi, 2014). A sizeable number of young people in Nigeria perceive Cybercrimes or internet scam as a means of sustenance. For instance, in 2019 alone, the High Court of Kwara State, Corams: Mahmood Abdulgafar and S. A. Oyinloye convicted numerous internet fraudsters (Tunde Oyekola**,** Kwara court jails Internet fraudster indicted by FBI, 2019).

It is no doubt that opportunities abound with the coming into existence of internet technology, advanced level of crimes are being perpetrated through this mechanism and this even posed

a danger to national security, (Samuel, Karina, Aderonke, Segun, 2019). Offences are being committed and culprits of these heinous crimes are labelled as'Yahoo boys'. It is axiomatic that the yahoo boys took advantage of cyberspace as offered by technology to swindle their innocent targets. These innocent targets are usually foreign nationals and the transactions are being carried-out with thousands and millions of dollars (Pulse ng: Court sentences yahoo boy to 35 years in prison, 25/06/2019). These yahoo boys usually present themselves as possessing specific items for sale or that they are into shipment of cargoes. Most of the culprits take advantage of some people eyeing for a wife or a husband via the internet (Amos,Internet fraud suspect wanted by FBI, sentenced to one year imprisonment in Ilorin, Oct. 17, 2019). These lawlessly minded persons will interact with the unsuspecting innocent persons via the internet, where they will pose as interested in relationship. Before the victim realized or knows what is happening, the offenders would have deceived them to credit them with dollars to facilitate travelling documents (Amos,Internet fraud suspect wanted by FBI, sentenced to one year imprisonment in Ilorin, Oct. 17, 2019). They fabricate documents and come-up with tales, beyond the imagination of the unsuspecting victims these victims often fell for the tales, thereby giving impression that yahoo boys have become successful in life.

In recent times, a story specified that Nigeria as a nation is losing about $ 80 million USD annually to software piracy (National Mirror Newspaper, May 22, 2013). The report was the discovery of a study concluded by the Institute of Digital Communication in South Africa. The American National Fraud Information Centre similarly stated that Nigerian money offers as the greatest online scam, up to 90 % in 2001(Maitanmi, 2014). The center also placed Nigeria cybercrime as being superbly high. For instance, e-mail spam and scams are the utmost hideous phenomena between the cybercrime, these are the coloration, which have been discovered to bean untrue financial investment. Nigeria's reputation is no doubt in question, because it has been degraded as a result of her citizens' involment in the cybercrime (Rushinek, A, Rushinek, SF, 1993). The criminals often send email stating that the victim is the named beneficiary to a will of estranged relative and stands to benefit the estate or the trust fund. Sometimes they used online charity and by this the offenders send email to the victims asking for funds and support to charitable organizations that do not exist.

Cyber Security and Human Rights Issue

Certain national and international legislators have made some attempt to look into human rights concerning cyber security standards. For instance, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Activists and others civil liberties were concerned with the impact that a wide cyber security regulations and codes could have on human rights (Electronic Frontier Foundation, 2013). "Human rights" here refer to rights protected under the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), which include, freedom of speech, freedom of expression, freedom of opinion, the right to privacy and freedom of association as some of the most basic rights of all humans. In reaction to the

foundation of the technology/Internet as an inventive platform for communicating essential human rights, the UN Special Rapporteur with regard to Freedom of Expression and free expression rapporteurs from Latin America, Europe and Africa signed a joint declaration affirming that "freedom of expression applies to the Internet" in 2011. Consequently, the UN Human Rights Council further in July 2012, established that "the same rights that people have offline must also be protected online," hence making the earlier stated human rights declarations of UDHR, ICCPR related to the Internet (John Perry Barlow, 1996).

The often proclaimed "Right to Internet" which allows individuals to have the right to internet when so desire and the "Right to be Forgotten" that guarantees that personal data remains personal and could be erased as may be desired, now form part of the general human rights principles relating to access to information (Jeff Jarvis,2010). Following the public outcry on cyber security, national autonomy, and individual freedoms to use internet over the years, in 2011, the UN Special Rapporteur on Freedom of Expression, Frank de la Rue from Guatemala, advised governments not to jettison those using internet from accessing it irrespective of the validation provided, inclusive of the ground of infringing right concerning intellectual property law. This is seen as a breach of article 19, paragraph 3, of the ICCPR. Frank de la Rue therefore called upon all states to make sure that access to internet is maintained at all times, even when there is political unrest (UN Doc. A/HRC/17/27, 2011).

It is beyond peradventure that cyber security extortions are genuine, the ability to communicate secretly, demonstrate, and have dialogue without being panic of intimidation is an essential element of human rights guaranteed to all people. There is therefore the need to balance this right with the sole aim of preventing cybercrimes and ensuring cyber security. This will further be discussed elaborately in the next part of this paper.

Selected Provisions of Nigerian Cybercrimes Act and Its Compliance with Human Rights Protection

The Cybercrime Act was enacted among others, for the detection, prevention and punishment of activities concerning cybercrimes. Prevention of cybercrimes will ostensibly involve clear risks of intrusions into privacy of citizens and restrict their freedom of expression or information in required cases (Giovanni Buttarelli, 2011). Therefore, it is central to take into account the civil liberties issues because the enforcement of cybercrimes law must be balanced with sufficient privacy and security consideration. Therefore, this part examines in detail the echelon of civil liberties of Nigerian citizens in the view of interpretation and implementation of specific provisions of part III of the Cybercrime Act. To achieve this, the discussion will be limited to those offences that constitute illegal activities under the Act. A careful look at the objectives of the Act shows that the paramount is the protection of significant information and cyber security. In fact reference is made to the need to protect privacy and intellectual property rights. This further supports the argument that the implementation of the Act must conform to the established international human rights treaties which will be examined in the course of discussing the Act (See section1 of the Act).

a) Child Pornography and Related Offences

In order to ensure the protection of a child, Section 23 of the Cybercrime Act makes the following offences punishable:

(a) Production and distribution of child pornography;
(b) Giving or making accessible child pornography;
(c) Releasing child pornography;
(d) Obtaining child pornography for another person or even oneself;
(e) In custody of child pornography in a laptop, on a computer-data storage medium or computer system;

Essentially, the essence of including the above offence in the Act is for the protection of the rights of a child as guaranteed in some notable international human rights instrument. A child is one of the vulnerable groups that have been victims of human rights violations that require special protection for the equal and effective enjoyment of their human rights. The protection of children rights have been spelt out in national and international human rights instruments and this show a sign of seriousness and attention to the plight of children. For instance, by the provision of Article 25 of the Universal Declaration of Human Rights (UNDHR) the right of children to adequate care and assistance and protection of their dignity are guaranteed. The UN Declaration of the Rights of the Child, 1948 noted in its preamble that states must ensure protection of children due to their mental and physical immaturity.

Thus, significant are the provisions of Article 23(4) and 24 of the (International Covenant on Civil and Political Rights 1966) ICCPR, which expressly refer to the rights of children including the adoption of appropriate steps by State party to make necessary provisions for the protection of the rights of children.

Of all the instruments on the rights of child, the UN Convention on the Rights of the Child 1989 is considered the most comprehensive of all instruments dealing with the protection of children rights (Francis, A. A., et al, 2010). This is owing to its universal recognition and adoption. The Convention sets out many rights already protected in other instruments such as UDHR, ICCPR, ICESCR and others. A child is defined in Article 1 of the Convention as any person below the age of 18 years unless under the law applicable to the child, majority is attained earlier. Similarly, in Africa, the Organization of African Unity (OAU) adopted the African Child's Right Charter in 1990 which entered into force in 1999. The Charter just like the UN Convention on the Right of a Child contains elaborate law for the protection of a child. These rights include, the right to life, the right to identify, the right to self-determination, the right against various abuses and many others (Article 2, 3, 4, 5 and 17 of the African Child's Rights Charter 1990). The World Health Organization Consultation on Child Abuse Prevention defines child sexual abuse to include child phonography in the following words:

> Child sexual abuse is the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or

> for which the child is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person. This may include but is not limited to: the inducement or coercion of a child to engage in any unlawful sexual activity; the exploitative use of a child in prostitution or other unlawful sexual practices; and the exploitative use of children in pornographic performance and materials.
>
> (World Health Organization, *Prevention of Child Abuse and Neglect Making the links between human rights and public health,* World Health Organization, 2001).

The above definition of a child who has been sexually abused given by the World Health Organization Consultation on Child Abuse Prevention is no doubt all inclusive. It looks at the child abuse further than the issue of having carnal knowledge of a child to include the use of a child for prostitution or oppressive engagement of children in pornographic act.

By year 2000, the Child's Rights Act was promulgated by the Nigerian National Assembly, following the Convention relating to the Right of the Child adopted by the UNGA in 1989 which was ratified by 192 countries (Achilihu, S. N, 2010). This was done in the spirit of the people Nigeria's tradition of struggling to ensuring meeting the desires of children as well as enhancing their welfare (Achilihu, S. N. 2010). This Act is an inclusion of all the rights concerning children and it considers all laws that provide for the right, protection and care of the children into a single legislation. This Act takes recognizance of the rights of children, self-esteem, restores their confidence and improves their statues. It equally makes children with disabilities to enjoy their rights fully as it makes provision for special measures to take care of their protection. It demands that in all actions concerning the child his or her best interest, welfare and well-being must be the paramount consideration (Adeyemi, A. A. 2003). Prevention of exploitation of children (Section 21 of the CRA, 2003), rendering of all child marriage void, (as a minimum age for marriage for female children is set at 18) are some of the uniqueness of the Act. Importantly, by the provision of section 31(1), no person is allowed to have sexual affairs with a child. Any person who breaches this provision an offence of rape and shall be liable upon conviction by the court to imprisonment for life (See section 31 (2)).

In addition, the legal right of children is also part of the provision in the Penal Code law. The Penal Code contains law that guards the rights of children. For example, section 237 considers the abandonment of a child whose age is below 12 years. Section 238 of the Act frown at cruelty to children and sections 271-280 take into account, abduction child, kidnapping and forced labour. There are equivalent provisions under the Criminal Code (Cap 42 Laws of Federation of Nigeria 2004).

Therefore, one can conclude the inclusion in the Cybercrimes Act for child phonograph is compatible with numerous instruments on the protection of child's rights. The significance of this is to prevent child abuse and exploitation.

b) Racism, Gender and Xenophobic Offences

Under the Cybercrimes Act, any person that share or makes available, gender, racist or any intolerant or xenophobic materials to individuals or the public by means of computer system against person(s) on the basis that they belong to a group and by reason of their sex, race, descent, colour, ethnicity or nationality has committed an offence. The word gender**,** racist, and xenophobic material as used in the Act means production of printed material which promotes hatred against individuals or group on the reason of their colour, nationality among others.

Importantly, the Cybercrimes Act prevents discrimination as stipulated in numerous national and international human rights documents. For instance, the African Charter in Article 2, prohibits discrimination of any kind. Article 3 envisages on equal treatment of all, while Article 5 forbids all kinds of inhumane, exploitation and debasing treatment. By Article 7, the Universal Declaration of Human Rights states that, everyone is equal in the eyes of the law and that all should be accorded the same protection against discrimination. In Nigeria, by section 42 of the Constitution, discrimination of whatever means is prohibited. Therefore, irrespective of your race, nationality, religion, no one must be discriminated against (the 1999 Constitution of the Federal Republic of Nigeria (as amended) 2011).

On this note, the Cybercrimes Act seeks to protect equality and equal treatment of person irrespective of where that person may reside or whatever their sexual orientation may be. Therefore, the Cybercrime Act is in line with the aspiration and objectives of the international human rights provisions.

c) Cyber Stalking and Terrorism

To ensure wide protection against all forms of cybercrimes, the Act makes provision for Cyber stalking which prohibits sending an insult, offensive or false message for the purpose causing annoyance (Section 15(1). The Cybercrimes Act also makes provision for Cyber terrorism and as such anyone who accesses or directs another to access any computer for purposes of committing terrorism has committed an offence (Alok Mishra and Deepti Mishra, 2008, p.217). Terrorism here denotes an illegal exercise of force or viciousness with in order to intimidate a government or member of the public on the reason of political or social purposes (Terrorism Prevention Act 2011).

The essence of the above is geared towards sufficient protection of the rights of person to life and liberty as protected in human rights documents. For example, section 33 of the Nigeria Constitution protects the life of everyone. The Constitution protects the right of everyone

to his personal liberty in section 35. So in this instance, act of terrorism is act capable of threatening the life of the people, and the constitution adequately makes provision for it. This act of terrorism also includes protection against any action capable of threatening life. Furthermore, protection against stalking is designed to protect the liberty of a person. Thus, act of stalking as prohibited in the Cyber Act is meant to safeguard the liberty of every citizens. This is because if not curbed, stalking is a form of defamation, which is capable of damaging the liberty and integrity of a person.

Unauthorized Access to a Computer

Concerning the access to computer, the Cybercrimes Act states that illicit or unauthorized opportunity to the use of a computer attracts punishment (Section 6(1) of the Act). For this reason, whoever make use of computer without authority or where such authority had been sought and obtained, but uses it in excess of that granted, intentionally accesses fully or partly, a computer system or other connected therewith is said to commit an offence. Where the provision of the law is breached with the intention of gathering data or confidential information, an offence with grave punishment as being committed (Section 6(2) of the Act). A vivid look at the later provision will reveal that accessing a computer with permission carries no liability. One question that one may ask here is that what if the person has acted ultravires though there was prior authorization. The Act has adequately envisaged this when it stated that the offence will be considered committed where a person has acted in excess of the authorization given to him (Section 6(3) of the Act). This shows that the mere fact that the there was a prior permission will not remove liability on the person.

Another aspect of unlawful access to computer that raises a human right issue is having access to the computer with the intent to obtain confidential information. The protection against this is to ensure that a person concerned is given absolute right to security of his or her information. This is in line with the provision of the Universal Declaration of Human Rights (Article 22) which protects the right to social security. Thus, the protection against unlawful access is akin to protecting social security of a person. Establishing intention is however, a question of fact and in most cases, it depends on the circumstance of the case.

Unlawful Interception

The Cybercrime Act 2015 has made provision for illegitimate jamming of communications and provides that whoever deliberately and with no permission or above the power, interrupts through mechanical medium, communications of content data or traffic data, non-public computer data 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 (Section 7 of the Act). The Act in this regard has made exclusion as to when a person will not be held liable. One of such is the presence of intention. By this particular

offence, the interception of public data is an offence and it is immaterial that consent is given. This means that this offence specifically relates to non-public computer data.

The protection against interception or jamming among individuals communications is to guarantee the right to privacy of a person. This right is protected for instance under the Universal Declaration of Human Rights (Article 12). The Article provides "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…" This shows that the Act is justified by making the interception of communications an offence in order to prevent arbitrary interference with the privacy of a person (Section 8 of the Act).

Similar to the right against unlawful interception of communications is the prohibition of destructing information. On this note, the Act makes it an offence to injure, destroy, erase, modify, or suppress a data with computer system (Section 8 (2) of the Act). It seems that the fulcrum of this prevision is to protect right to property as stipulated in some international human rights treaties. For instance, Article 17 of the Universal Declaration of Human Rights guaranteed the right to everyone to own property and that no one should be deprived of his property except in accordance with the order of the court e.g. execution ordered by court to satisfy judgment debt. Therefore, the prohibition of destructing information as provided in the Act is to ensure and protect property right of a person. It is important to state that that a destruction of information with regard to computer or any data held therein is said to have occurred in the following instances (Section 8 (3) of the Act):

(i) where a program or data in a computer is altered or erased;
(ii) where a program or data in a computer is included or removed; or
(iii) where the act occurs that impairs the ordinary operation of any computer concerned.

The above are instances where the right to property can be said to have been violated under the Act.

Computer Integrity Offences

These are major crime acts focused at integrity, confidentiality and accessibility to certain critical information (Section 3 and 5 of the Cybercrimes Act, 2015). The essence of this crime is to guide against unlawful access to national critical information. There seems to be two variable rights that this offences seeks to protect. First is the right of person to receive information and the second is the right of the government to protect critical information by not making it available to the public. For instance, the Universal Declaration of Human Rights (Article 19) gives everyone the right to freedom of expression, which indeed includes the right to receive, search and pass information. The human right to information, for instance, is guarantee but it must not violate the dignity or privacy of others. Also, if personal information concerning health status of family is accessible for everyone, it goes without saying that this information violates the rights of the family concerned. This means

that access to critical information capable of damaging the reputation of a person must not be disclosed. The aspect that requires balancing here is how to strike equilibrium between the right to a state to withhold critical information and that of the individual to receive information. It is on this basis that the Act stipulated that certain critical information must not be made accessible to the public and even where accessible to a person, it must not be disclosed. The disclosure of such information will attract a grave punishment under the Act.

System Interference

The Cybercrimes Act protects the content of computer system. The essence of this is to prevent unlawful interference with the computer system of a person. This is very germane in the protection of the right of a person to the fullest enjoyment of their right to privacy without arbitrary interference (Section 9 of the Act). For instance, the Nigerian Constitution in section 37 guaranteed the right of every person to privacy which in this case includes, the right to receive correspondence without interception, family life and their homes. Therefore, any interference into the computer system of a person is a grave violation of this right.

Identity Theft and Impersonation

Concerning the impersonation and identity theft, the Act makes provision in this regard and in addition provides that whoever in the process of using computer system or any other connected thereto is said to have committed an offence if (Section 13 and 14 of the Act):

(a) Intentionally obtains another person's identity or information with the intention of deceiving or defraud, or
(b) Dishonestly impersonates another person, whether is living or dead, with the intention of -
    (i) gaining advantage either for himself or another person;
    (ii) obtaining any property or interest thereon;
    (iii) causing disadvantage to the person being misrepresented; or
    (iv) avoiding arrest or prosecution and perversion of the course of justice.

Essentially, the above provision is geared towards ensuring protection of liberty and security of individuals in accordance with some international human rights documents. For instance, Article 1 of the American Declaration of Rights and Duties of Man guarantees the right to life, liberty and security person (American Declaration of Rights and Duties of Man 1992). In the same vein, the African Charter on Human and Peoples' Rights also contain similar provision in Article 6 that "every individual shall have the right to liberty and to the security of his person". Also in Article 4, the Charter provides that "every human being shall be entitled to respect for his life and the integrity of his person" (African [Banjul] Charter on Human and Peoples' Rights, 1981).

However, there seems to be a defence with respect to this particular offence. This is because it impersonation and identity theft will only be an offence under the Act if it is committed with the intention to deceive, defraud, or gain advantage. Therefore, where the purpose of interference is not with these intentions, the offender will not be liable. However, such offender may be liable under the Act for accessing a computer without permission. This is even more so that to succeed in a case of human rights abuse, it is not the law that the victim must have suffered any personal injury. Therefore, a mere interference will suffice here.

Conclusion

This paper has examined the link between cyber security and protection of civil liberties. The examination revealed that while protecting the cyber space, it is desirable to bear in mind the internationally recognized rights. The paper has also looked into the details of offences created under Cybercrimes Act and their significance in the protection of internationally recognized rights. It revealed how to balance prevention of cybercrimes with the right of an individual to enjoy his or her right to privacy and at the same ensuring cyber security. It was observed in this paper that there seems to be two variable rights which the legislature seeks to protect. On one hand, it seeks the right of person to receive information and on the other hand, it considers the right of the government to protect critical information by not making it accessible to the public.

References

Achilihu, S. N. (2010). *Do African children have rights? A comparative and legal analysis of the United Nations Convention on the Rights of the Child*. Universal-Publishers. Retrieved from http://books.google.com/books?hl=en&lr=&id=V9ICUHILa68C&oi=fnd&pg=PA9&dq=Child+Rights+Convention+Muscroft+%22General+Assembly%22&ots=Ln9Jlkcf6r&sig=7pErYMcKKWerPBk2vD33w9GNugI

Adeyemi, A. A. (2003). Child Rights Promotion in Nigeria: An Overview. A UNICEF, sponsored study on the Child's Rights Act.

African [Banjul] Charter on Human and Peoples' Rights, adopted June 27, 1981, *entered into force* Oct. 21, 1986.

American Declaration of Rights and Duties of Man 1992

Amos Abba, Internet fraud suspect wanted by FBI, sentenced to one year imprisonment in Ilorin, Oct. 17, 2019) https://www.icirnigeria.org/internet-fraud-suspect-wanted-by-fbi-sentenced-to-one-year-imprisonment-in-ilorin/ accessed on 17/12/19.

Article 2, 3, 4, 5 and 17 of the African Child's Rights Charter 1990

Awang Dzul-Hashriq Dharfizi, The Energy Sector and the Internet of Things – Sustainable Consumption and Enhanced Security through Industrial Revolution 4.0, Journal of International Studies Vol. 14, 99-117 (2018), p.99

Business and Human Rights Resource Center, 'Ranking Digital Rights project': http://www.business-humanrights.org/Documents/Ranking_Digital_Rights (Access December 2013).

Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%20 14%20- %20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a CorporealEnvironment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489; *Goodman*, Why the Policy don't care about

Child Rights Act 2003

Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

Constitution of the Federal Republic of Nigeria 1999 [as amended] 2011.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). See also the Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), Strasbourg, 28.I.2003.

Court Jails Two Fraudsters in Ilorin, https://efccnigeria.org/efcc/news/5254-court-jails-two-fraudsters-in-ilorin accessed on 17/12/19.

Court sentences yahoo boy to 35 years in prison, https://www.pulse.ng/news/local/court-sentences-yahoo-boy-to-35-years-in-prison/2de7b5y accessed on 17/12/19.

Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

Cyber warfare and Nigeria's National Security. (2013). Retrieved from http://www.thisdaylive.com/articles/cyber-warfare-and-nigeria-s-national-security/148887/

Cybercrimes Act, 2015.

Elbit Systems officials arrive, begin installation of $ 40 million internet spy facility for Nigeria. (2013, 26 Nov). Retrieved from available https://www.premiumtimesng.com/news/150333-exclusive-elbitsystems-officials-arrive-begin-installation-40-million-internet-spy-facility-nigeria.html.

Electronic Frontier Foundation, 'Internet Surveillance and Free Speech: The United Nations Makes the Connection' 4 June 2013. https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection (Access December 2013).

Florida Cyber-Security Manual, Secure Florida, November 2004, p. 150. Available from secureflorida.org.

Francis, A. A., Adekunle, G. S., Michael, S. A., & others. (2010). Law and children's rights protection: The Nexus for a Sustainable Development in Nigeria. Canadian Social Science, 6(2), P26–33.

Giovanni Buttarelli, 'European Data Protection Supervisor': Security and civil liberties in the fight against cybercrime fundamental legal principles for a balanced approach' (2011).

Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

International Covenant on Civil and Political Rights 1966.

Jeff Jarvis 'A Bill of Rights in Cyberspace', 27 March 2010, http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace.

John Perry Barlow, 'A Declaration of the Independence of Cyberspace' 8 February 1996. https://projects.eff.org/~barlow/Declaration-Final.html (Access December 2013).

MaitanmiOlusola, 'Impact of Cyber Crimes on Nigerian Economy', the International Journal of Engineering and Sciences (IJES) Volume 2, Issue 4, p. 47. ISSN 2319-1813. Available at. http://www.theijes.com/papers/v2-i4/part.%20%284%29/H0244045051.pdf. Accessed on 3/2/2014.

Mishra, A., & Misra, D. (2018). *A summary of the legislation on cybercrime in Nigeria*. (2018). Retrieved from https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria&option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria

Office of the High Commissioner for Human Rights, *Human Rights Indicators: A Guide to Measurement and Implementation* (Geneva: 2013) https://unp.un.org/Details.aspx?pid=23745 (Access December 2013); For the definition of digital rights.

Optional Protocol to the Convention on the Rights of the child on the sale of children, child prostitution and child pornography adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May,2000 and entered into force on January 18, 2002 and Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict adopted and opened for signature ratification and accession by General Assembly resolution A/RES/54/263 of May 25th, 2000. It entered into force on 12 February, 2002. http:///www.unhehr.ch.lhtml/mean3/b/treaty/7.htm.

Oyenike Mary Olanrewaju & Faith Oluwatosin Adebiyi. (2014), The impact of mobile information and communication technology on cybercrime in Nigeria. *International Journal of Engineering Research & Technology (IJERT)*, Vol. 3 Issue 8, August, p.586.

Rushinek, A, Rushinek, SF. "Using Experts for Detecting and Litigating Computer Crime". Managerial Auditing Journal. 8.7(1993):19-22; Simpson, Doug. "Feds Find Dangerous Cyber stalking Hard to Prevent". 12 June 2000. http://archives.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/index.html

Samuel Oni, Karina Araife Berepubo, Aderonke Atinuke Oni, Segun Joshua. (2019). E-government and the challenge of cybercrime, 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG) 24-26 April 2019.

Terrorism Prevention Act 2011

Tunde Oyekola, Five jailed for internet fraud in Kwara, https://punchng.com/five-jailed-for-internet-fraud-in-kwara/ accessed on 17/12/19.

Tunde Oyekola, Kwara court jails Internet fraudster indicted by FBI https://punchng.com/kwara-court-jails-internet-fraudster-indicted-by-fbi/ accessed on 17/12/19.

UN Convention on the Rights of the Child 1989

UN Declaration on the Rights of the Child 1959.

UN Doc. A/HRC/17/27. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, para.23, 79.

Wihbey J. *Global Prevalence of Child Sexual Abuse,* available on http://journalistsresource.org/studies/government/criminal-justice/global-prevalence-child-sexual-abuse

World Health Organization, *Prevention of Child Abuse and Neglect Making the links between human rights and public health,* World Health Organization, 2001.