A CRITICAL APPRAISAL OF THE CYBERCRIMES ACT, 2015 IN NIGERIA[1]

BY

OLANREWAJU ADESOLA ONADEKO[2]

And

ABRAHAM FEMI AFOLAYAN[3]

ABSTRACT

The digital and information technology age has created new avenues and tools for committing traditional crimes and new forms of crimes. The architecture of the digital world challenges law enforcement institutions and the criminal justice system to device measures and procedure to contend with digital or cybercrimes. In Nigeria, there had overtime been a significant increase in internet-based advance fee fraud. There are cases of hacking into emails, website and infringement on privacy rights of persons and institutions which call for urgent solution.

Legislation on advance fee fraud is among the earliest intervention by the Nigerian Government on cybercrimes, but the law is inadequate to meet the intricacies of technological development. The most recent statute on cybercrimes in Nigeria is the Cybercrimes (Prohibition and Prevention etc) Act, 2015. The vaunted objectives of this Act include the provision of an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act is designed to ensure the protection of critical national information infrastructure and to promote cyber security, protect computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. This paper reviews the provisions of the Act and identifies its strengths and weaknesses.

The Act is not without some loop-holes and need urgent amendment. It unnecessarily limits its scope to the protection of Critical National Information Infrastructure and does not sufficiently provide for the broad framework, which is the key objective of the Act. It is the suggestion herein that the Act be amended to include areas not related to Critical National Information Infrastructure.

INTRODUCTION

The use of information and communication technology (ICT) which currently dominated our daily lives and economic interactions has led to an increase in cybercrimes in the form of

[1] Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada July 24 – 28, 2016.

[2] Olanrewaju Adesola Onadeko is the Director-General, Nigerian Law School, Bwari, Abuja, Nigeria.

[3] Abraham Femi Afolayan is a Director (Academics), Nigerian Law School, Bwari, Abuja, Nigeria.

hacking, infringement of intellectual property, credit card theft, phishing, spamming, cyber-stalking, cyber-squatting, illegal access to data, misuse of computer devices for fraud, cyber terrorism and other forms of online crimes. The use of internet has reduced the whole world to a global village as we are able to connect and interact with one another and transact businesses across borders and physical territories. The global nature of the internet makes it easy for a criminal armed with a computer and the internet to victimise individuals and businesses anywhere in the world right inside his home.[4] Nigeria has joined the global community by enacting the Cybercrime (Prohibition, Prevention etc) Act, 2015 (hereinafter referred to as "the Act") on May 5, 2015 with the aim of securing our cyber space. The Act contains 59 sections, 8 parts and two schedules. The First Schedule provides for members of the Cybercrime Advisory Council while the Second Schedule provides for businesses to be levied for the purpose of Cyber-security Fund.

The aim of the Act is to provide an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act is also intended to ensure the protection of Critical National Information Infrastructure, and promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[5] However, prior to the enactment of the Act, the Advance Fee Fraud and Other Related Offences Act, 2006, the Economic and Financial Crimes Commission (EFCC) Act, 2004 and the Money Laundering Act, 2012 regulated cybercrimes in Nigeria. These legislations were inadequate and that was the reason why the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 was made. In the case of *Harrison Odiawa (alias Abu Belgore)* v. *Federal Republic of Nigeria*,[6] a syndicate used the internet to defraud an American citizen of USD 2 million. The offenders were tried under the Advance Fee Fraud and Other Related Offences Act, 2006. The first defendant was sentenced to twelve years imprisonment on each of the four counts without an option of fine while the second defendant was sentenced to ten years imprisonment on each of the three counts without an option of fine. It was not that Nigeria had no law on cybercrime but the Act was made to cope with the advancement of technological growth and the complexities involved in the investigation and prosecution of cybercrime and internet based offences.

What is cybercrime?

The Act failed to define "cybercrime," however attempt will be made here to define it. Cybercrime may be described as an act that involves the use of computers, network or electronic information technology devices or the internet to perpetuate criminal activities like illegal access to data,[7] data interference,[8] system interference,[9] computer related fraud and forgery,[10] misuse of

[4] Prof. Bolaji Owasanoye, "Information Technology and Criminal Justice Administration" (2010) NLRJ 13 at 20.
[5] See the explanatory memorandum attached to the Act.
[6] [2008] 57 WRN 83
[7] See sections 6, 28(3), 5 and 31 of the Cybercrimes (Prohibition, Prevention etc.) Act, 2015.
[8] *ibid* section 16.

devices for crime,[11] illegal interception, intellectual property violations, terrorism and viral attacks. Any crime committed in the cyberspace is a cybercrime; or put in a more succinct way, any crime committed by using computer as a tool for the perpetration of the offence can generally be described as a cybercrime. Such act includes hacking, cracking, stalking, squatting, phishing, identity theft, impersonation, spoofing, software piracy, credit card fraud and viral attacks through the use of computers.[12]

Section 258 of the Evidence Act, 2011 (Nigeria) defines "computer" as any device for storing and processing information. Also, section 58 of the Cybercrimes Act defines "computer" as:

> an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols.

THE OBJECTIVES OF THE ACT

The objectives of the Act are to:

> (a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
>
> (b) ensure the protection of critical national information infrastructure; and
>
> (c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[13]

The Act is a federal enactment and it is applicable throughout Nigeria.[14] It thus appears that no State House of Assembly can legislate on cybercrime to protect the cyber space and security in the state. Where such law is made, it must be in conformity with the provisions of the Act.[15] The Criminal Law of Lagos State Cap. 41, 2011 provides for offences relating to misuse of computer

---

[9] *ibid* sections 8 and 16.
[10] *ibid* sections 13 and 14.
[11] *ibid* sections 18, 24 and 25.
[12] E. Onoja, Fundamental Principles of Nigerian Criminal Law, Green World Publishing Company Ltd, 2015 page 607 - 608
[13] Section 1 of the Act.
[14] Section 2 of the Act
[15] See section 4(5) Constitution of the Federal Republic of Nigeria, 1999 (as amended) which provides for the doctrines of covering the field.

and electronic data which predated the Cybercrime Act, 2015 but this law is only applicable in Lagos State.

PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

The Act provides for the protection of Critical National Information Infrastructure.[16] Critical infrastructure is defined in section 58 of the Act as:

> systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country.

Section 3 (1) of the Act empowers the President of the Federal Republic of Nigeria through the recommendation of the National Security Adviser, by Order published in the Federal Gazette to designate certain computer systems and networks whether physical or virtual as Critical National Information infrastructure.

The information must be so vital to the country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.[17]

The Order made by the President may prescribe minimum standards, guidelines, rules or procedure in respect of protection or preservation and general management, access to or control of critical information infrastructure. The aim of this section generally is to protect Critical National Information Infrastructure from any form of interference by cybercriminals. It is pertinent to note that the provisions of section 3 of the Act remain inchoate until an order made by the President is published in the Federal Gazette.

OFFENCES AND PENALTIES UNDER THE ACT:

(i) **Offences against Critical National Information Infrastructure –** Section 5 of the Act provides that any person who with intent, commits any offence against the critical national information infrastructure designated pursuant to section 3 of the Act, shall be liable on conviction to imprisonment for 10 years without option of fine. Where the offence committed results in grievous bodily harm to any person, the offender shall be liable on conviction to imprisonment for 15 years without option of fine.[18] Where the offence committed results in death of person(s), the offender shall be liable on conviction to life imprisonment.[19] The provision of section 5 of the Act is made pursuant to section 3 of the Act. That is to say, this provision is

[16] See sections 3 and 4 of the Act.
[17] Section 3 (1) of the Act.
[18] *Ibid*, section 5 (2) of the Act
[19] *Ibid*, Section 5 (3)

effective only when the National Security Adviser has made a recommendation to the President of the Federal Republic of Nigeria designating some computer systems and networks as critical national information infrastructure and the President acting on this recommendation will make an order published in the Federal Gazette in this respect. There is presently no gazette containing such an order.

(ii) Unlawful access to a computer – Section 6 (1) of the Act makes it an offence for any person without authorisation to intentionally access in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security. It is also an offence to intentionally obtain computer data, secure access to any program, commercial or industrial secrets or classified information.[20] It is an offence under the Act to unlawfully intercept data[21] or to either directly or indirectly modifies or causes the modification of any data held in any computer system or network by way of alteration, erasure, removal, suppression or prevention of the normal operation of the computer system or network.[22] It is an offence to use any device for the purpose of avoiding detection or otherwise prevent identification or attribution with any of these acts or omissions.[23]

Section 6(4) makes any person or organisation who knowingly and intentionally trafficks in any password or similar information through which a computer may be accessed without lawful authority which affects public, private and or individual interest in and outside Nigeria an offence.[24] It should be emphasised that this provision is applicable extra-territorially. The effectiveness of its implementation depends on Nigeria maintaining international cooperation with member states.

The Act prohibits disclosure of access codes or passwords for an unlawful purpose.[25] The Act also prohibits illegal retrieval of passwords of gaining access fraudulently through automated means.[26] The Act mandates employees to surrender access codes upon disengagement.[27]

(iii) **Registration of Cybercafe** – The Act provides that all operators of cybercafé shall register with the Computer Professionals' Registration Council and also register their business names with the Corporate Affairs Commission (C.A.C). The operators shall maintain a register of users through a sign-in register which shall be made available to law enforcement personnel whenever it is required.[28] It should be noted that the Act did not expressly provide for any law enforcement

[20] *Ibid*, section 6 (2)
[21] *Ibid*, section 12 (1)
[22] *Ibid*, section 16 (1)
[23] *Ibid*, section 6 (3)
[24] *Ibid*, section 6 (4)
[25] Ibid, Section 28 (3)
[26] *Ibid*, section 28 (5)
[27] *Ibid*, section 31
[28] Section 7(1) of the Act.

authority to be in charge of ensuring compliance with this provision. Thus, there may be difficulties in monitoring and enforcing compliance of this provision.

Section 7(2) makes it an offence for any person to perpetrate electronic fraud or online fraud using a cybercafé. The Act also makes it an offence for the owners of cybercafé to connive with the offenders.[29]

(iv) **System Interference –** Section 8 of the Act makes it an offence for any person without lawful authority to cause any computer from functioning by way of inputting, transmitting, amaging, deleting, deteriorating, altering or suppressing its data in order to prevent the computer from functioning in accordance with its intended purpose.

Section 16 prohibits unauthorised modification of computer systems, network data and system interference. Section 13 of the Act makes it an offence to be engaged in forgery by making inauthentic data to look as if it is authentic or genuine. Section 17(1)(c) of the Act makes it an offence for any person to be engaged in the forgery of another's signature or a company's mandate.

Section 14 of the Act makes it an offence to be engaged in computer related fraud. It provides that any person employed by or under the authority of any bank or other financial institutions who with intent to defraud, directly or indirectly diverts electronic mails shall be guilty of an offence and on conviction, shall be liable to imprisonment.[30] Section 14(4)(b) of the Act makes a very interesting provision which is novel in the Nigerian Criminal Law which states that a person convicted of fraud shall in addition to the term of imprisonment refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or customer. The victim of crime may have to institute a civil action for damages or compensation before restitution can be made.

(v) **Intercepting Electronic Messages, E mails and Electronic Money Transfers** – Section 9 of the Act makes it an offence for any person to destroy or abort any electronic mails or processes through which money or any valuable information is being conveyed. The Act did not provide for the definition of what constitute "valuable information" thereby making its interpretation subjective. Section 19 of the Act imposes a duty on financial institutions to safe guard sensitive information of their customers. The section prohibits them from giving a single employee access to sensitive information. Financial institutions are to provide effective counter-fraud measures to safeguard their sensitive information. Where there is a case of negligence of duty, the Act places the burden of proof on the customer to establish that the

[29] Section 135(2) Evidence Act places the burden of proof of criminal offences on person who alleges that an offence has been committed. By section 139 Evidence Act, such offence must be proved beyond reasonable doubt.

[30] See section 14 (4)(a) of the Act

financial institution in question should have done more to safeguard its information integrity.[31] The Act makes it an offence for employees of financial institutions from issuing false electronic or verbal messages with intent to defraud.[32] Section 22 of the Act makes it an offence to be engaged in identity theft and impersonation of any person engaged in the services of any financial institution.

(vi) **Cyber terrorism** – Section 18 of the Act makes it an offence for any person to access or cause to be accessed any computer or computer systems or networks for purposes of terrorism. The punishment for this offence is life imprisonment. For the purpose of this section "terrorism" shall have the same meaning and effect as contained in the Terrorism (Prevention) Act, 2011 (as amended).[33] The Act also makes it an offence for a person to be engaged in cyberstalking[34] that is the act of sending to someone offensive materials to cause fear by means of computer system or network. The court may make an order to stop the harassment of the person concerned.[35] The Act also makes it an offence for a person to be engaged in cybersquatting.[36] That is the acquisition of a domain name on the internet in bad faith purposely to profit, mislead, destroy reputation or to prevent others from registering the same name which is so similar, identical, or confusing to an existing trademark registered with appropriate government agency at the time of the domain name registration.[37] This section protects intellectual property rights on the internet and cyberspace.[38]

Section 32 of the Act makes it an offence to be engaged in phishing and spamming and the spread of computer viruses. Phishing is the act of fraudulent means of acquiring sensitive information such as usernames, passwords and credit card details through the e-mails or instant messaging system from banks or financial institutions.[39]

(vii) **Stealing of electronic devices** – Section 15 of the Act makes it an offence for any person to be involved in stealing or attempt to steal financial institutions or public infrastructure terminal or Automated Teller Machine.

(viii) **Child pornography and abuse** – Section 23 of the Act makes it an offence for any one using computer system or network to engage in child pornography or engage in sexual activities of a child who is below the age of 18 years in any computer system or network.[40] It has been opined that this provision will cover the use of social media such as Facebook, Twitter,

[31] See section 19 (3) of the Act
[32] *Ibid*, section 20
[33] *Ibid*, section 18 (2)
[34] *Ibid*, section 24
[35] Ibid, section 24 (3)
[36] *Ibid*, section 25
[37] Ibid, section 58.
[38] Ibid, section 25 (3)
[39] Ibid, section 58
[40] Ibid, section 23 (1)(3)(5)

Instagram and other social media, from meeting a child and engaging in sexual activities and transmitting same through portable hand set and other communication devises that would qualify as a computer system under section 58 of the Act.[41]

ADMINISTRATION AND ENFORCEMENT PROCEDURES

Section 41(1) of the Act provides that the office of the National Security Adviser (NSA) shall be the coordinating body for all security and enforcement agencies under the Act. The NSA is to provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria. Its other duties are to:

- Ensure formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria;
- Establish and maintain a National Computer Emergency Response Team (CERT) Coordination Centre responsible for managing cyber incidences in Nigeria;
- Establish and maintain a National Computer Forensic Laboratory and coordinate utilization of facility by all enforcement, security and intelligence agencies;
- Build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under the Act or any other law on cybercrime in Nigeria;
- Establish appropriate platforms for Public Private Partnership (PPP);
- Coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security; and
- Do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under the Act.

It is the duty on the Attorney-General of the Federation to strengthen and enhance the existing legal framework to ensure the conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards. The Attorney-General is to ensure the maintenance of international cooperation required for preventing and combating cybercrime and promoting cyber security. He is to ensure effective prosecution of cybercrimes and cyber security offenders.[42] Section 57 of the Act empowers the Attorney-General of the Federation to make rules, regulations, subsidiary legislation and cure any lacuna by way of regulation for the purpose of efficient implementation of the provisions of the Act.

The Act requires all law enforcement agencies involved in the enforcement of the Act to organise training programs for officers in charge of prohibition, prevention, detection, investigation, and prosecution of cybercrimes.[43]

[41] Oluwakemi Oluwafunmilayo Oke in her article entitled "An appraisal of the Cybercrime (Prohibition Etc) Act, 2015, pages 10 – 11;
[42] Section 41 (2) of the Act
[43] Ibid, section 41 (3)

Section 42 prescribes the establishment of the Cybercrime Advisory Council to be presided over by the National Security Adviser. The Council is to meet at least four times a year for members to share knowledge and promote the study of cybercrime detection. This provision if properly implemented will update the knowledge of officers engaged in the implementation of the Act. Through this provision, members can also interact and exchange ideas that will benefit others in the system.

Section 44 of the Act provides for the establishment of National Cyber Security Fund where a levy of 0.005 of all electronic transactions by businesses specified in the second schedule to the Act, gifts and grants will be kept. Such businesses includes GSM service providers and all telecommunications companies, internet service providers, banks and other financial institutions, insurance companies and the Nigerian Stock Exchange.

Section 45 of the Act gives power to the law enforcement officer to apply to court by way of ex-parte application for a judge to issue a warrant of arrest, search warrant and seize, remove or detain anything which contains evidence of the commission of an offence under the Act. Under section 46 of the Act, it is an offence to obstruct any law enforcement officer in the discharge of his duty under the Act.

Section 48 gives the court power to order a person convicted of an offence under the Act to forfeit to the Government of Nigeria any proceeds from the offence. If the convicted person has assets in foreign countries, subjects to treaties between Nigeria and such foreign countries, such assets shall be confiscated to the Government of Nigeria. Section 49 of the Act provides that a convicted person may be compelled by order of court to make restitution to the victim the proceeds of crime.

It is the duty of any one operating a computer system to notify the National Computer Emergency Response Team (CERT) of any attacks or intrusion on its computer and failure to report the crime constitutes an offence under the Act and the convict is liable to pay fine.[44] The Act did not specify how and where CERT will be contacted and the procedure for laying such complaint.

JURISDICTION AND INTERNATIONAL COOPERATION

Section 50 of the Act confers jurisdiction over offences committed under the Act on the Federal High Court. The action may be commenced in any Federal High Court in Nigeria regardless of where the cause of action arose. This provision contradicts the decision of the Court of Appeal in the case of *Ibori* v. *Federal Republic of Nigeria*[45] where it was held that a defendant must be tried where the incident that led to his trial took place. Section 52 of the Act provides that

[44] Ibid, section 21
[45] [2009] 3 NWLR (Pt. 1127) 94

offences under the Act shall be extraditable under the Extradition Act.[46] Section 53 provides that evidence obtained in a foreign country can be used in court proceedings in Nigeria provided such evidence is authenticated by a judge, magistrate or justice of peace or by a seal of a Ministry or Department of the Government of a foreign state. Section 56 provides that the National Security Adviser shall make available a contact point twenty four hours every day for countries that have entered into agreement or treatise with Nigeria.

PITFALLS AND RECOMMENDATIONS

(a) The Act creates several offences without adequate stipulation for the enforcement of provisions. It has already been pointed out that the Act did not specifically confer power on any law enforcement agency to enforce the provisions of the Act. There is no clear cut body to report incidents of infringements or file petitions. There is the need to decentralise and distribute enforcement framework with a view to providing clarity as to the law enforcement agencies responsible for enforcements of specific provisions of the Act.

(b) There are so many provisions in the Act which contradict other laws made by the National Assembly, e.g. the burden of proof required under the Act is on the preponderance of evidence. Most of the offences created under the Act are criminal in nature and the standard of proof ought to be proof beyond reasonable doubt, which is the standard required under the Evidence Act, 2011.

(c) The Act attempts to regulate the activities of banks and financial institutions in Nigeria; whereas such acts are already regulated by the Banks and Other Financial Institutions Act. The Act also attempts to regulate the services of service providers, whereas, such acts are already regulated by the Nigerian Communication Commissions Act. The duplication may create challenges for the courts when confronted with deciding which Act is applicable in a given situation.

(d) The implementation of the Act requires international cooperation with other nations, whereas, Nigeria at the moment is not a signatory to any cybercrime convention. It is advised that Nigeria should be a signatory to the Budapest Convention on Cybercrime to enhance its international cooperation in combating cybercrime.

(e) As already pointed out, sections 3 and 4 of the Act provides for the protection of National Information Infrastructure. The President of the Federal Republic of Nigeria acting on the recommendation of the National Security Adviser is by order empowered to publish in the Federal Gazette and designate some computer systems and networks as Critical National Information Infrastructure. This is the foundation upon which the Act is built, but sadly, there is no order published in the Federal Gazette designating any computer systems or networks as Critical National Information Infrastructure.

[46] See Cap E25 Laws of the Federation of Nigeria, 2004.

The National Security Adviser should be advised to urgently recommend to the President, the computer systems or networks that will constitute Critical National Information Infrastructure, to enable the President make an order in this respect.

(f) The Act provides for the Attorney-General to make rules and regulations supplementary to the Act as guidelines for acting on reports, detection, investigations and prosecution of offences under the Act. So far, but such directive has not been implemented by the office of the Attorney-General of the Federation in line with the provisions of the Act.

CONCLUSION

The Act is a good law if properly implemented. Nigeria is advised to enter into international treaties and conventions on cybercrime to be able to enjoy international cooperation as this law cannot be effective without the cooperation of other nations in the world.

The National Security Adviser should recommend to the President the computer systems and networks that should be designated as Critical National Information Infrastructure. The Attorney-General of the Federation should on his part provide guidelines for the rules and procedure for acting on reports, investigation and prosecution of cybercrime offences.

Finally, there should be a definite direction on the implementations of the Act by the law enforcement agencies. The Act should be amended to give specific roles to each law enforcement agency on their roles in the execution of the provisions of the Act.

If the recommended adjustments are considered and effected, the Act will be on its way to providing an efficient legislative framework for the curtailment of cybercrime in Nigeria.