AN ASSESSMENT OF NIGERIA'S CYBERCRIMES (PREVENTION, PREVENTION ETC.) ACT 2015

Oluwaseun Viyon Ojo, Lagos State University

Available at: https://works.bepress.com/oluwaseun_ojo/9/
AN ASSESSMENT OF NIGERIA’S CYBERCRIMES (PROHIBITION, PREVENTION ETC) ACT 2015

Baron Verulam of Verulam and Viscount of St. Albans 1561-1626 (English philosophers) once said that "Crime is always a by-product of an innovation or invention". With the advent of computers, the internet and various technological innovations, there arose monstrous criminal and anti-social activities perpetrated by several criminals on unsuspecting users on these huge technological resources. It must be noted that cybercrime is one of the teething problems amongst others of the invention and introduction of technology and computer into the society. As much as the advent of technology has brought about speed, ease and breadth in the exchange of information within and without borders, it has indirectly and undeniably brought about the invention of modern-day crimes which were not known to or covered by the existing criminal legislations in Nigeria. The absence of a definitive legal machinery in Nigeria to provide for and tackle the pervasive problem of cybercrime has generated sustained and vociferous clamour from all quarters both from the Information and Communications Technology (ICT) sector and the legal community for a concrete and comprehensive legal, regulatory and institutional framework for dealing with the supposed hydra-headed problem of cybercrime.

In response to the various requests and demands from concerned stakeholders in both the ICT and legal sectors, former President Goodluck Jonathan, at the twilight of his administration, signed into law the Cybercrime (Prevention, Prohibition etc.) Act on May 15, 2015. The Act on that day entered into the corpus of legislations validly in force within the Nigerian legal system. Thus, the principal aim of this piece is to examine and assess the key and notable provisions of the Cybercrime (Prevention, Prohibition etc.) Act.

Before delving into the examination of this Act, I consider it apposite to explain what cybercrime is. In simple, compact terms, cybercrime is any crime that involves a computer and a network. D C Debarati Halder and Dr. K. Jaishanker (2011) define cybercrime as “offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss, to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”. Cybercrimes usually threaten a nation’s security and financial health. As a matter of fact, cybercrimes sometimes transcend the national border of a country as it often involves the interests of at least another nation state. Thus, criminal activities perpetrated on the internet range from fraud, theft, pervasive pornography, child pornography, paedophile rings, drug trafficking, extortion, hacking, copyright infringement, plagiarism, child grooming, cyber stalking, cyber warfare, cyber terrorism, to mention a few.

With the above foundation about cybercrime properly laid, attention will now be turned to the key and pivotal provisions of the recently enacted Cybercrime (Prevention, Prohibition etc.) Act 2015 dealing with the vexed issue of cybercrime. It must be quickly mentioned here that the Act has been long awaited in Nigeria in view of the drift of the Nigerian commercial environment from paper-based transactions to paperless transactions and the continual entrenchment of electronic commerce in the various sectors of the economy. As such, this Act will particularly provide for all the possible issues of crimes and anti-social activities accompanying the emerging electronic commerce economy as well as putting in place appropriate punitive measures for all conceivable cybercrimes in Nigeria.
The lofty objective of the Act was laid down in section 1 thereof. Without doubt, the real purpose and intention of the Act is clearly discernable from this provision of the Act. Thus, the Cybercrimes (Prohibition, Prevention etc.) Act 2015 creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters. Particularly, the Act engenders a platform for cyber security and in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information.

Designation and Protection of Critical National Information Infrastructure

In view of the critical and detrimental effect of cybercrimes on the state of security and financial health of a nation, the President, by virtue of section 3(1) of the Act, may, on the recommendation of the National Security Adviser designate by order published in the Federal Gazette certain computer systems, networks and information infrastructure vital to the national security of Nigeria as well as her economic and social being, as constituting Critical National Infrastructure. By section 4 of the Act, the presidential order may require the office of the National Security Adviser to audit and inspect any Critical National Information Infrastructure at any time to ensure compliance with the provisions of the Act. Pursuant to the above, the Act prescribes different penalties for any contravention of the provisions of the Act pertaining to Critical National Information Infrastructure ranging from 10 years without option of fine, 15 years without the option of fine to life imprisonment see section 5 (1)(2) and (3) of the Act.

Furthermore, any person who accesses without authorisation, any computer system or network for fraudulent purposes and also obtains data which is vital to national security, is liable on conviction to a term of not more than 5 years or to a fine of not more than N5,000,000,000 or both. Any unlawful system interference for fraudulent purposes by deleting, transmitting, damaging or suppressing computer data which prevents the system from functioning, is liable on conviction to a fine of N5,000,000 or imprisonment for a term of not more than 2 years or both. This is provided for under section 8 of the Act.

Designation of Offences under the Act

The Cybercrime Act lists offenses and penalties including unlawful access to computers; unlawful interceptions of communications; unauthorised modification of data; misuse of data; system interference; intercepting electronic messages, emails, e-money transfer, tampering with critical infrastructure; computer related fraud; computer related forgery, among others, as offenses that are punishable under the Act. Theft of electronic devices, electronic signature, child pornography and related offenses, racism and xenophobic offenses are also punishable under the Act. It also provided for cyber-stalking, cybersquatting and cyber-terrorism as offenses.

Cyber-stalking as provided under the Act includes the use of the internet or other electronic means to stalk or harass an individual, a group of individuals or an organisation. It may include false accusations, monitoring, making threats, identity theft and damage to data or equipment, the solicitation of minors for sex or gathering information in order to harass. Also, it includes sending multiple e-mails, often on a systematic basis, to annoy, embarrass, intimidate, or threaten a person or to make the person fearful that he/she or a member of his/her family or household will be harmed. Thus, any person who, by means of a public electronic communications network, persistently sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent or he knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent commits an offence and shall be liable on conviction on conviction to N2,000,000 or imprisonment for not less than one year or to both.

Also, any person that accesses or causes to be accessed any computer or computer system or network for purpose of terrorism commits the offence of cyber-terrorism and will be liable on conviction to life imprisonment. Terrorism, as used here, shall have the same meaning under the Terrorism (Prevention) Act, 2011 (as amended).

Regulation of Financial Institutions Use of Electronic Transactions

In addition and on an important note, the Act imposes a duty of care on financial institutions to their customers to put in place effective checks against cybercrimes. Section 37 (1) of the Act provides that a financial institution “shall verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuing ATM cards, credit cards, debit cards and other related electronic devices”. An official or organisation who fails to obtain proper identity of customers before executing customer electronic instructions in whatever way commits an offence and is liable on conviction to a fine of N5,000,000. This is well provided for under section 37 (2) of the Act.

This provision seems to provide a proper check against identity theft on the account of customers which is becoming increasingly prevalent in the financial sector. In other words, it will ensure that financial institutions, where banking transactions are taking place, put in place an effective bulwark against financial malpractices. This provision will usher in a new dawn in electronic commercial transactions in the financial world most especially in respect of the duty of care imposed on the financial institutions.

Retention of Records by service providers and disclosure/interception of electronic communication

The Act, by virtue of section 38(1) of the Act, provides that a service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority (in this case the Nigerian Communications Commission), for the time being responsible for the regulation of communication services in Nigeria for a period of two years. Additionally, having due regard to an
individual’s right to privacy under the Constitution of the Federal Republic of Nigeria Cap C23, Laws of the Federation of Nigeria 2004, service providers shall at the request of the relevant authority release any information required to be retained. (See section 38(5) of the Act).

Furthermore, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purpose of a criminal investigation or proceeding, a judge may, on the basis of information on oath order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data or traffic data associated with specified communications transmitted by means of a computer system, (see section 39 of the Act).

Establishment of the Cybercrime Advisory Council and the National Cyber Security Fund

The Act establishes the Cybercrime Advisory Council (the Council), which shall amongst other functions provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria. See Section 43(1) of the Act.

Additionally, the Act establishes the National Cyber Security Fund (the "Fund"), which shall be domiciled with the Central Bank of Nigeria and wherein shall be paid a levy of 0.05 of all electronic transactions by the business specified in the schedule of the Act, grants-in-aid and assistance from donor, bilateral and multilateral agencies; all other sums accruing to the Fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organisations (provided such monies as may be appropriated for the Fund by the National Assembly and all other monies that may, from time to time, accrue to the Fund. See Section 44 (1) of the Act. The monies accruing to the Fund is exempted from income tax while all contributions to the Fund is tax deductible. (See section 44(3) of the Act).

This paper merely highlights the key provisions of the Act and it does not appear to be an exhaustive one. Just as it has been long awaited in the Nigeria criminal justice system, it is hoped that the Act will come to play an important role in the administration of justice. Now, the court can particularly define the nature of offences relating to computer and the internet and determine the appropriate penalty as against speculating on what offence a person should be convicted under the old criminal codes. Thus, the coming into effect of the Act should usher in a concrete and comprehensive legal framework for cybercrimes and other related offences in Nigeria. It is therefore suggested here that all relevant stakeholders in the legal community, ICT and financial sector must work collaboratively to ensure the full implementation of the Act and fully realise its lofty objectives.

Ojo Oluwaseun Viyon

Ojo Oluwaseun Viyon is a graduate of law from Lagos State University (LASU), Lagos, Nigeria.

Author: tlc

302 articles / Browse all articles

RELATED ARTICLES »

AN XRAY OF NIGERIA’S CYBERCRIMES ACT 2015 VIS-À-VIS THE RIGHT TO PRIVACY
THE INTERNET, FREE SPEECH AND NATIONAL LAWS
ELECTRONIC SERVICE OF COURT PROCESSES IN AFRICA: HOW RELEVANT IS FACEBOOK, YAHOO AND GM?