HEADWATERS
"Integrity. Experience. Solutions"

OVERVIEW OF THE CYBER CRIME ACT 2015

In an increasingly digitalized, globalized and technological skyrocketing World, the extent of computer related crimes both locally and globally is reaching mammoth proportions.

There is a revolution going on in criminal activity. The revolution lies in the way that networked computers permits crimes to be committed remotely. A criminal no longer needs to be at the actual scene of the crime to prey on his victim as the world is now a global community interlinked by computer devices.

A full appreciation of this paper will be built on a working definition of Cyber crime. Halder, D., & Jaishankar, K. 2011 in their book Cyber crime and the Victimization of Women: Laws, Rights, and Regulations defined the term 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 to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.

In Nigeria, the Cyber Crime (Prohibition, prevention etc) Act enacted in May 2015 was the first legislation for the regulation of cyber space in the Country as similar offences in times past were prosecuted under the criminal code, EFCC act and other similar anti-graft agencies Act.

The explanatory memorandum of the Act captures its relevance as it provides thus:

"The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights."

The objectives of the Act are to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; 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.

Key areas of the Act are Provision of a Remedial Benefits for victims of Cybercrimes Activity, requirement for the registration of all Cyber Café's in Nigeria, Creation of an advisory council, Creation of a Cyber security fund and the protection of critical information infrastructure.

The Act makes provisions for cyber security and safety in Nigeria, notable among them is the designation of certain computer networks as "**Critical National Infrastructure**" provided for under section 3 of the legislation. It is quintessential to state that the term is used to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for electricity, gas production, telecommunication health, agriculture etc. Flowing from this, section 5(3) of the Act provides that any unauthorized access of the **computer networks** designated as critical National Infrastructure attracts a punishment of Life imprisonment for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual (amongst other punishments for lesser crimes).

In its bid to meet up with challenging global cyber trends, In addition to the above, The President may designate other computer networks as Critical National Infrastructure based on the recommendations of the National Security Adviser in line with the Provisions of the Act.

In addition, the Act provides for a wide range of cyber offences including but not limited to Unlawful access to a computer, Intercepting electronic messages, emails, electronic

money transfers, Willful misdirection of electronic messages, Computer related fraud, Theft of electronic devices, Unauthorized modification of computer system, network data and system interference, Fraudulent issuance of e-instruction, Identity theft and impersonation, Child pornography and related offences, Cyber stalking, Cyber squatting, Racists and xenophobic offences, Attempt, conspiracy, aiding and abetting, Manipulation of ATM/POS Terminals, Phishing, spamming and spreading of computer virus and Electronic card related fraud

Specifically, Section 32 of the Act criminalizes the offence of Phishing and spamming and the spread of computer virus. Phishing is defined under the Act as the criminal and fraudulent process of attempting to acquire sensitive information such as usernames and password.

Section 33 of the Act deals with electronic cards and related fraud, the section attempts to criminalize any act of tampering with credit, debit, charge and other types of financial cards. The section criminalizes the act of stealing an electronic card.

Section 33(13) imposes a duty on financial institutions to make available to the Central Bank of Nigeria or a licensed credit bureau which seeks to determine only the cardholders rating without the permission of the cardholder but must within 7 working days give notice in writing of the disclosure to the cardholder failure to notify the card owner within the stated period, such financial institution commits an offence.

Section 34 criminalizes the act of dealing with another person's card.

Section 35 criminalizes the act of selling by an unauthorized person of cards and purchase of such cards. Section 36 of the Act criminalizes the use of fraudulent device or attached emails to obtain information or details of a cardholder.

A notable provision is section 26 which criminalizes the sharing/publication of racist and Xenophobic materials by a Person or group of persons via a computer or justifies acts constituting genocide or crimes against humanity, Commits an offence and shall be liable

upon conviction to imprisonment for a term of not more than 5 years or to a fine of not more thanN10,000,000.00 or both such fine and imprisonment.

The Act specifically prohibits the sharing of nude, pornographic, offensive contents or menacing characters also known as cyber stalking. Offenders shall according to Section 24 (b) of the Act be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

Similarly, Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and shall be liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than N5,000,000.00 or to both fine and imprisonment.

The Act places stringent punitive measures on cyber terrorism as it provides under section 18 (1) that Any person that accesses or causes to be accessed any computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment. Terrorism used under this Act has the full implication as Terrorism under the Terrorism (prevention) Act 2011 as amended.

The Act as part of its mandate established a Council Known as the Cybercrime Advisory Council under section 42 which is expected to amongst other things provide recommendations on issues relating to the prevention and combating of cybercrimes and related criminal activities in Nigeria comprising of representatives from all the security agencies in the country which shall be actively coordinated by the National Security Adviser.

To nip cyber fraud in the bud, the Act imposes a duty on Financial institutions to 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 issuance of ATM cards, credit cards, Debit cards and other related electronic devices; and prescribes a fine of N5,000,000 (Five million naira) for failing to verify an online transaction.

In the tenor of the Act, section 37 (3) provides as follows:

"Any financial institution that makes an unauthorized debit on a customers account shall upon written notification by the customer, provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours. Any financial institution that fails to reverse such debit within 72 hours , shall be guilty of an offence and liable on conviction to restitution of the debit and a fine of N 5, 000,000.00."

The implication of the above is an imposition of a duty of due diligence on financial institutions in Nigeria. Additionally, Section 40 of the Act imposes a duty on the service provider to work with Law enforcement agencies and prescribes it as a criminal offence for failure to do so.

Section 27 (2) provides that any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

Unfortunately, the perpetrators of cybercrime still launder proceeds gotten from their unsuspecting victims through these financial institutions.

This provision also stretches the regulatory powers of the Act to the operations of Banks and Financial Institutions whose operations are already governed by the Central Bank of Nigeria Act and the Banks and Other Financial Institutions Act herein referred to as (BOFIA). This creates an overlap in the applicability of the Acts. The Banks and Other Financial Institutions Act has placed the supervision of Banks and Financial Institutions under the purview of the Central of Bank Nigeria. Section 33 of BOFIA gives the Governor

of Central Bank the power to order a special examination or investigation of the books and affairs of a Bank where he is satisfied that it is in the public interest to do so or the bank has been carrying on its business in a manner detrimental to the interest of its depositors and creditors. Hence the provisions of the cybercrime Act that regulates the relationship of financial institutions with its customer is inconsistent with the provisions of BOFIA.

On the issue of Jurisdiction of court to enter cyber related offences, Section 50 of the Act vests jurisdiction over offences committed under the Act on the Federal High Court regardless of where the offence is committed in Nigeria, in a ship or aircraft registered in Nigeria, by a citizen or resident in Nigeria if it would constitute an offence under a Law of the Country where the offence was committed, or outside Nigeria where the victim of the offence is a citizen or the alleged offender is in Nigeria and not extradited. This raises conflict of Law issues as it is against the established principle of International Law that a criminal be prosecuted where the offence is committed.

This looming legal tussle has been settled by the provision of section 51 which provides that offences created under the Act shall be extraditable under the Extradition Act. Thus, offenders in Nigeria can be extradited back to the host country where such cyber crime was committed subject to whether or not the host country has a treaty or reciprocal arrangement with Nigeria.

The Cybercrime Act establishes several criminal offences but did not make adequate provisions as to the mode of enforcement of its provisions. The Act also failed to state in detail the Law enforcement agencies that will be in charge of enforcement of the provisions of the Act. Although it imposes a duty on the office of the National security Adviser to be in charge of the enforcement of the provisions of the Act the definition section defines Law enforcement agencies to include “such agencies that will be in charge of enforcement of the provisions of the Act”. There should be clarity as to the Law enforcement agencies that

are in charge of the enforcement of the provisions of the Act as Nigeria has several law enforcement agencies.

Another enforcement challenge posed by the Act, is the international outlook of cybercrimes which makes it necessary for international cooperation by various nations of the world to tackle cybercrime. Presently, Nigeria is not a signatory to any cybercrime convention, which makes International cooperation harder. There is need for Nigeria to become a signatory to the Budapest Convention on Cybercrime

The Act also attempted to regulate service providers whose conduct has also being regulated by the Nigerian Communications Commissions Act and the regulations made pursuant to it, although the Act can be read alongside with the regulations made pursuant to the Nigerian Communications Commissions Act.

CONCLUSION

The enactment of the Cybercrime (Prohibition Prevention etc.) Act in Nigeria is a good step in the right direction but the Act has several loopholes and lacuna which if not addressed would make the Act one of the many dead Laws in the Nigerian statute books.
It is important that the Attorney General of the Federation should make rules and regulations which will be supplementary to the Act to provide for appropriate guidelines for detection, handling of reports, investigation, and prosecution of offences under the Act. Also there is need for international cooperation by the Law enforcement agencies of the Act with other Law enforcement agents in other Nations to appropriately deal with Cybercrime in Nigeria.

Author : Adedamola Victor Kuforiji

HEADWATERS LEGAL ADVSIORY

4TH FLOOR ELDER DEMPSTER BUILDING

CENTRAL BUSINESS DISTRICT

47 MARINA LAGOS