CYBERSECURITY: *Are Fintech & I. T. Gurus Cyber-Criminals Under the Ambit of the Law?*

Introduction

The perception of the Nigerian cyber infrastructure and the legal apparatus for the sustenance and governance of the cyber space, is one which has been largely left in the dark, as such enough misconceptions abound as to trending legal and socio-economic issues arising in respect of cyber security.

One of such misconceptions, presently rocking the Nigerian social corridors is whether or not the average IT enthusiasts and IT professionals walking our streets, who concern themselves with digital technologies, coding, web development, software development, ethical hacking, graphic designs, and a host of others are cyber criminals within the context of the Nigerian laws?

It is kindly observed, that although a host of handlers of the cyber space in Nigeria employ their level of technological expertise to indulge the cyber environment in furtherance of their malicious intent and purposes, to commit frauds and other unlawful acts, this should not make the entirety of our IT professionals criminals under the intentions of our laws.

Are Cyber Space Operators, Criminals in the Eyes of the Law?

To set this discuss in the right perspective, it is imperative to state clearly that social opinions and perceptions do not amount to what is legally right or wrong, as the above is strictly within the confines of cold laws and fact, and as such, are not subject to the dictates of social opinions, assertions, arguments and conclusions. They are governed by the provisions of the laws in force, which govern such areas of humanity and the ability of the Courts, to give meaning to the relevant laws, in the light of facts before it thereby determining the fate of the individuals before it and doing justice.

The issue of whether or not, a cyber-operator is a criminal, or guilty of a crime or not, is strictly governed by the existing laws, enforcement processes and legal frameworks. The provision of the Constitution of the Federal Republic of Nigeria,1999(as amended), being a chief actor in the totality of Nigeria's Criminal justice administration, has laid the above to rest, where it provides quite unequivocally under Section 36 (5) that:

> *"Every person who is charged with a criminal offence shall be presumed to be innocent until he is proved guilty."*

And Section 36 (11) of the Constitution, where it states clearly:

> *"a person shall not be convicted of a criminal offence unless that offence is defined and the penalty therefore is prescribed in a written law, and in this*

subsection, a written law refers to an Act of the National Assembly or a Law of a State, any subsidiary legislation or instrument under the provisions of a law".

By the combined construction and deduction of both provisions above, a person, can only be declared a criminal, when the Courts make a pronouncement to that effect, in the light of the relevant statutory provision, defining such act, as an offence and punishing it.

In addition to the above existing legal foundations for criminal enforcement in Nigeria, our criminal justice administration, has laudably evolved to meet the demands of cyber security, through the recent enactment of the **Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015,** which has clearly defined and punished a wide variety of cyber-offences, all in a bid to make the cyber space a better place, including but not limited to cyber stalking, bullying and terrorism, to mention but a few.

In recent days, the Court of Appeal, in the case of **Solomon Okedara V. AGF *(2019) LCN/12768 (CA)***, had to consider the Constitutionality of **Section 24** of the Cybercrimes Act to determine whether or not such was inconsistent with the overriding provisions of the Constitution.

The above Section, provides:

> *"A person who knowingly or intentionally sends a message or other matter by means of computer systems or network that is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be sent, or he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent, commits an offence under this Act and is liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term not more than 3 years or both."*

In determining the constitutionality of the above provision, The Court reasoned from the above provision that the legislature has the power to enact laws that are reasonably justifiable in a democratic society and that such laws shall not be declared invalid merely because they appear to be in conflict with the rights and freedom extended to citizens under the Constitution. However, the Court noted, for example in the case at hand, that the right of freedom of speech guaranteed under **Section 39** cannot be taken away "except for the purposes of preserving the interest of defence, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons."

Thus, the question of whether a person is a cyber-criminal or not, is exclusively determinable by the Courts, when the Courts breathes life into the provisions of the Cybercrimes Act and other existing legal frameworks relevant to the Nigerian cyber space. Today, the Act, has defined and punished several acts which are capable of being committed on the online space, including:

- **Section 18,** Cyber Terrorism,
- **Section 22,** Identity Theft and Impersonation
- **Section 23,** Child Pornography and Related Offences,
- **Section 23(2)** Cyber Bullying
- **Section 24,** Cyber Stalking,
- **Section 25,** Cybersquatting, to mention but a few.

It is therefore clear, that IT gurus and Fintechs, are not cybercriminals within the ambit of our laws, in the event that the society wrongly terms them as such, they only become criminals, when the Courts pronounces them as such and does justice in the light of relevant and pre-existing legal frameworks.

Cyber Space Operators and Law Enforcement Agencies: Towards a Mutually Beneficial Partnership

As the Fin-Tech and IT industry continues to grow and develop, so does the opportunities for criminals to exploit such systems meant to foster innovation as well. Thus, it is important to have that trust and collaboration between regulators, enforcement agencies and Fintech companies through establishing better lines of communications and also getting involved in their regulations by reporting violators, operate according to standards and confines of the law, host workshops and symposia regularly.

Establishing an open channel of communication, is imperative to enhancing legal collaborations and partnership, which helps to secure productive platforms of curbing the events of criminality in our cyber space, For the following reasons;

1. The availability of the requisite skills and technical know-how among cyber space operators, could help beef up the apparatus of

the Nigerian law enforcement agencies, towards better cyber space policing.

2. The operators of the Nigerian cyber space, could help make reports of any suspicious occurrences among the cyber space operators, capable of evolving into cybercrimes.

3. The Nigerian law enforcement agents, can better leverage on indigenous cyber space organisations, bodies and associations, to report acts of misconduct or ethical breaches, among their members, thereby curbing potential threats to the security to the Nigerian cyber space.

4. The law enforcement agents, could better curb the menace of cybercrimes, by engaging cyber operators within their ranks thereby enhancing the efficiency of cyber policing.

The Emerging Fields of Cyber Threats: A Wake-up Call for Nigerian Cyber Space Protection

While it is laudable, that the Nigerian criminal justice system has set in motion a legal framework for managing and controlling the events of cyber-crimes within her borders, through her recognition and enactment of the **Cyber Crimes Act, 2015**, it is imperative to note that law exists as a tool of social engineering and must continually evolve to meet the emerging curves that hampers man's existentiality, by the constant review, amendment and if need be, enactment of new and relevant laws, which tackle emerging trends in crime commission in the cyber space.

It is also important for cyber space law enforcers, to be fully abreast with this emerging tendencies and potentials in the cyber space today to adequately build capacity and enforce sanity in the cyber space. Among the emerging areas of cyber threats are:

a. **Identity Theft:** This has become very prevalent in Nigeria. Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and the end result is that victims are typically left with damage to their credit, finances, and reputation.

b. **Ransomware:** This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code. Most ransomware is delivered via malicious emails.

c. **Hackers:** Gaining access to IT systems from outside an organisation still offers rich pickings for criminals. Traditionally they have attempted to gain access to bank account information or credit card databases. However, intellectual property is another source of value. The use of social engineering, tricking staff into revealing user names and passwords, remains a threat.

d. **Data leakage:** While cyber security in the office may seem challenging, it is essential to understand that security extends well beyond the office these days. The use of smart phones and tablets has become widespread. The ubiquitous and cheap nature of portable storage devices makes them a useful tool for the backup and transportation of data. Those features mean they are also a target for data thieves.

e. **Malware on Mobile Apps:** Mobile devices are vulnerable to malware attacks just like other computing hardware. Attackers may embed malware in app downloads, mobile websites or phishing emails and text messages. Once compromised, a mobile device can give the malicious actor access to personal information, location data and financial accounts.

f. **Phishing:** An email-borne attack that involves tricking the email recipient into disclosing confidential information or downloading malware by clicking on a hyperlink in the message.

g. **Spear Phishing:** A more sophisticated form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.

h. **Cyber Espionage:** Both large and small organizations are beginning to store at least some of their data in the cloud. Right Scale recently found that private cloud adoption increased to 77% among organizations; hybrid cloud computing increased as well. Whether the thief is coming from the inside or outside, attacking private, public or hybrid cloud technologies, trade secrets and other valuable intellectual properties are at risk. This is, of course, in addition to valuable customer data.

Conclusion

Conclusively, it is kindly observed that the Nigerian cyber policing infrastructure, must develop competence, in the light of the recent emerging issues and threats which are presently exasperating the Nigerian cyber space. It is in not enough that there are laws, and legal frameworks recognising and curbing the events of cybercrimes in Nigeria. Our cyber security enforcement frameworks, must treat the commission of cyber offences differently in the light of enabling legislations, expertise, technical know-how and experience, and awake to the demands of cyber security, policing and enforcement, when this is done, the issues of cyber security will be brought to a definite rest.

Author

O. M. Atoyebi, SAN
Managing Partner, Omaplex Law Firm
atoyebi@omaplex.com.ng

Contributors

Isaac Adeyanju
isaac.adeyanju@omaplex.com.ng

Caleb Echoga
caleb.echoga@omaplex.com.ng