JOURNAL OF JURISPRUSDENCE, INTERNATIONAL LAW AND CONTEMPORARY LEGAL ISSUES
Rivers State University, Faculty of Law *ISSN: 1115 5167 Vol.18 Issue.1, 2024*

CURBING INTERNET CRIMES IN NIGERIA: NEED FOR THE RESTORATION OF INTERNET INTEGRITY

By

Joshua Uba, Esq[1]

Abstract:
The internet is just like a very big and busy market; it has several kinds of activities going on at the same time. No doubt, the internet has transformed the entire world into a global village and made interactions between individuals and entities unrestricted by borders and geographical delimitations, resulting in increase in trade, tourism, and communication among others. However, the internet is not without its downsides to humanity. It has not only created novel crimes but has also been employed in aid of the commission of various crimes. This article gives a critical inroad on the relevance of the internet to humanity in modern times, analyses its downsides, evaluates the legal implications and dynamics of the same and finally makes a case for the restoration of its integrity.

Keywords: *Crimes, Internet Crimes, Internet Integrity*

1.0 Introduction

The internet is a global system of interconnected networks of computers and other communication devices that make use of standardized communication protocols to link devices worldwide to provide a variety of information and communication services[2]. It can also be referred to as the cyberspace[3].

With the internet, the ‘’global village concept’’ is made possible with seemingly impossible interactions made attainable leading to enhanced trade, tourism, communication among others. On the downside, the internet has created unique challenges, mostly hitherto unknown but for the internet. The internet has not only created novel crimes, but it is also being employed in aid of the commission of various crimes. According to Akinwunmi,[4] the challenges of cybercrimes like invasion of privacy, election meddling, hate speech, fake news, and dissemination of obscene content globally all gained momentum because of the internet.

Integrity,[5] on the other hand, entails the quality of possessing and steadfastly adhering to high moral principles or professional standards. In other words, a thing could be said to possess integrity if it adheres to moral principles and can be said to be of a high standard with respect to its composition. Thus, people and things lacking acceptable standards and principles are said to be without integrity. From the above, it is safe to posit that the internet without integrity entails the internet being deprived of its morality, standard and safety nets hence deliberately compromising its generally accepted

---

[1]Joshua Obinna Uba is a Google Policy Fellow. (emeritus) and presently works as the State Program Manager (Access to Justice) of the Pub;ic and Private Development Centre. . He can be reached on joshuauba22@gmail.com
[2] National Information Technology Development Agency (NITDA). "NITDA Framework and Guidelines for Public Internet Access." Title of the Code of Federal Regulations, vol. 1, NITDA, Year.
[3] Akinwunmi, Akinkunmi. *The Nigerian Internet Law*, Ciplus Limited, 2019.
[4] Ibid
[5] *Encarta World English Dictionary.* Bloomsbury Publishing PLC, 1999, p. 974.

standard as a medium meant to assist and enhance interaction for communication and other gainful purposes.

A meticulous observance of the trajectory of the development of the various compositions of the internet beginning from 1962 J.C.R Licklider's famous memo ''The Galactic Network''[6] Concept to the introduction of the email in 1972 to the present progression from first generation to fifth generation Wireless Network (5G), a recurrent truth that runs through is the intention of the movers to create a medium laden with integrity and only for the best purposes for mankind.[7] To drive home this point is the case of the infamous 9/11 attack at the World Trade Center, USA. The terrorists hijacked and diverted some aircraft from their scheduled purpose, routine and route and instead moved them to hit their target causing pain and harm to humanity. That is totally an abuse of the purposes of those aircraft. Of course, the aircraft manufacturers, when building, never planned to build a medium for terrorists to hijack and cause mayhem to mankind. At that moment, the terrorists abused the use and purpose of the aircraft and one can say the aircraft were manipulated to lose their integrity as a means of conveying passengers safely from one point to another. This is exactly what happens whenever the internet is manipulated to soothe the selfish desires of its users and of course this leads to losses of both human and financial resources by the victims.

There has been heightened outrage over the surge of internet abuse in Nigeria. Daily, cyber fraudsters, otherwise known as 'Yahoo Boys' are twirling their victims of their hard-earned money. In fact, it has taken a worse turn as some wicked ones employing the internet technology, especially the social media, have reportedly not only raped their victims but murdered some in cold blood[8]. Internet abusers are hoodwinking their culprits through fake news, hate speech, cyber bullying, phishing, cyber stalking etc.

2.0 History of Internet in Nigeria

Despite its long existence in other climes, internet usage commenced in Nigeria in 1991[9] with just a few pioneering groups offering limited email services[10] to some privileged Nigerians. The worldwide web became available in Nigeria in 1996 while comprehensive internet services became available in 1998[11] but was only assessed at cyber cafes. Quite recently, due to the liberalization of the telecommunications sector, advancement and availability of internet enabled mobile phones at affordable prices the rate of internet connectivity quadrupled. Despite her late embrace of the internet, Nigeria has the highest number of internet users and penetration in Africa.[12] This might not be unconnected with our large population size and the other factors already outlined necessitating the embrace of the internet in the country.

[6] The concept discussed is a network of computers that allows users to gather data and accesses programs anywhere in the world.
[7] For more on this, see Akinkunmi, Akinwunmi. *The Nigerian Internet Law*, Ciplus Limited, 2019, pp. 25-26.
[8] Omole, Ibukun. "Ritual Killings, Internet Fraud: Need for National Reorientation." *Punch Newspapers*, 20 Feb. 2022, http://www.https://punchng.com/ritual-killings-internet-fraud-need-for-national-reorientation/. Accessed 14th Nov. 2023.
[9] Eshekels Associates. "Trends in Internet Usage in Nigeria." *Information and Communication Technologies (ICT's) Resource and Research Centre*, 2001.
[10] Email was introduced globally in 1972.
[11] Adomi, E. E. "Internet Development and Connectivity in Nigeria." *Program: Electronic Library and Information Systems*, vol. 39, no. 3, 2005, p. 257.
[12] Akinkunmi, Akinwunmi , *The Nigerian Internet Law*, Ciplus Limited, 2019

2.1 Legal and Policy Regime of Internet Integrity in Nigeria

It is the view of some that legal and regulatory framework to protect the integrity of the internet as to curb against cyber fraud started late in Nigeria[13] because at the onset, the attention and focus of the government and indeed stakeholders was on penetration, building digital infrastructures, regulation, and licensing of internet service providers (ISP's). Little or no concern was placed on the mode of use by the end users of the internet. This led to a mass abuse of the internet for fraud and criminal activities, especially for the young and unemployed who saw the internet as a bailout of the vicissitudes of life and succor to make ends meet illegally. It is reported that between 2000 and 2013, Nigerian banks lost approximately N159 billion to cyber frauds[14]. Foreigners, especially the female gender, were at the receiving end and in most cases got lured to part with huge amounts of money. However, despite the seeming setback, Nigeria today apart from a body of robust policy framework has the Cybercrimes (Prohibition, Prevention) Act 2015. Other laws that govern the internet in Nigeria are the Economic and Financial Crimes Act, the Independent Corrupt Practices and other Related Offences Act, the Criminal Code, the Penal Code, the National Security Adviser's Act, the Nigerian Communications Commission Act, the Freedom of Information Act, the 1999 Constitution as amended, the Nigeria Information and Technology Act, amongst others.

Apart from the laws, there are also policies and drafts like the Internet Code of Practice, Consumer Code of Practice Regulations (CCPR), the General Code of Practice, Quality of Service Regulations. The framework and guidelines for public internet access among others is to uphold internet integrity and ensure an efficient internet network in Nigeria. However, even with the existence of these laws, policies and regulations, there seems to be an escalation of the abuse of the internet these days, especially social media. There has been a tremendous decline in the integrity of the internet, leading to perceived extreme reactions by the Government to regulate citizen's time online in the form of the Social Media Regulation Bill.[15] For a guarantee of continuous and uninterrupted access to the internet, it is pertinent users learn to uphold the integrity of the internet by resisting the temptation of using the internet as a medium to perpetuate crime and engage in unbecoming acts.

2.2 Likely Conduct that Rob the Internet of its Integrity and Current Legislative Responses Therein

As said earlier, though not at par with some other jurisdictions and contrary to the belief of many, there exist laws[16] and regulations aimed at upholding the integrity of the internet, discourage internet crimes and ensure the safety of internet users. This being the case, the need for the proposed 'Social Media Regulation Bill' seems to be watery. As a free and democratic nation, citizens' right to express themselves with civility already guaranteed by the constitution[17] should not be trampled upon, especially when there are pieces of legislation in existence that seems to address the identified gaps. We shall attempt to discuss a few of them.

[13] USA enacted her first law (18. U.S.C 1030) to address computer related abuses.
[14] *National Mirror*, Lagos, 4 September 2015, http://nationalmirroronline.net/new/experts-list-benefits-of-cybercrime-law-to-nigeria-economy/. Accessed 3 November 2023.
[15] The proposed Social Media Bill which sought to gauge social media was heavily resisted by Nigerians.
[16] Cybercrimes Act, Part III.
[17] Constitution of the Federal Republic of Nigeria (CFRN) 1999, as amended, sec. 36.

1. Electronic or Cyber Fraud Through Cyber Café

By virtue of S. 7 (2) of the Cybercrimes Act, it is an offence to perpetrate an electronic or online fraud using a cybercafé. By S. 7 (3) of this same law, the owner of a cybercafé will be deemed to have committed an offence where he connives with the perpetrator of a cyber fraud.

2. Sending Electronic Messages with the Intent to Defraud

Section 14(2) of the Cybercrimes Act makes it an offence to send electronic messages with the intent to defraud the recipient or another person. The sent messages may represent facts or sets of facts that can cause damage or loss when relied upon by the recipient or another person. An example is phishing that involves sending unsolicited and malicious emails by online fraudsters to hoodwink the recipients or using social media platforms to send unsolicited messages in disguise of one's identity or in misrepresentation of facts to the recipient.

i. Forging of Electronic Signature

By virtue of section 17 (3) of the Cybercrimes Act, it is an offence to forge another person's signature or company mandate through electronic devices with the intent to defraud or cause misrepresentation.[18]

ii. Cyber Terrorism

By virtue of section 18 (1) of the Cybercrimes Act, any person that accesses or causes to be accessed any computer system or network for terrorism commits an offence. Section 18 (2) of the Cybercrimes Act adopts the definition of terrorism as defined under the Terrorism (Prevention) Act 2011.

Section 1 (2) of the Act states among others that ''act of terrorism '' means an act done deliberately with malice, aforethought and which.

a) may seriously harm or damage a country or an international organization.

b) is intended or can reasonably be regarded as having intended to -unduly compel a government or international organization to perform or abstain from performing any act.

c) involves or causes, as the case may be-an attack upon a person's life which may cause serious bodily harm or death; or destruction to a government or public facility, an infrastructure facility, including an information system, a public place or private property, likely to endanger human life or result in major economic loss; and

d) an act or omission in or outside Nigeria which constitutes an offence within the scope of counter-terrorism protocols and conventions duly ratified by Nigeria.

The United Nations Security Council defined it as:

Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the public or in a group of

[18] Upon conviction, the offender is liable to imprisonment for not more than 7 years or a fine not exceeding N10,000,000.00 or both

persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act[19].

A cyber terrorist upon conviction is liable to life imprisonment.[20]

3. Identity theft and Impersonation

Section 22(2) of the Cybercrimes Act makes it an offence to fraudulently use the electronic signature, password, or any other unique identification feature of another person. It is also an offence to fraudulently impersonate another entity or person, whether living or dead.[21] For someone to be convicted of this, the person must have committed the offence with the intention to gain an advantage for himself or another person; obtain any property or an interest in any property; cause disadvantage to the entity or person being impersonated or another person; or avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.[22]

4. Child Pornography

A child or a minor is defined as a person below 18 years of age.[23] Section 23 (1)(a)–e of the Cybercrimes Act makes it an offence to produce, offer or make available, distribute or transmit, procure for oneself or another and possess child pornography in a computer system or a computer data storage medium. The Act[24] states that child pornography includes pornographic materials that visually depict a minor being engaged in sexually explicit conducts, a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct. Upon conviction, a convict could spend up to ten years in jail.[25] By virtue of Section 23 (2) of the Cyber Crimes Act, it is an offense for any person to make or send other pornographic images to another computer by way of unsolicited distribution. The offender upon conviction shall be sentenced to 10 years imprisonment or a fine of N20,000,000.00 or both.

5. Cyber stalking

Section 58 of the Cybercrimes Act defines cyber stalking as a course of conduct directed at a specific person that would cause a reasonable person to feel fear. Section 46 of the Violence Against Persons (Prohibition) Act (VAPP) 2015 defines stalking as

a) Watching or loitering outside or near the building or place where such person resides, works, carries on business, studies, or happens to be; or

b) Following, pursuing, or accosting any person in a manner that induces fear or anxiety.

Examples of stalking include making threats against someone or that person's family or friends; non-consensual communication such as repeated phone calls, emails, text messages, unwanted gifts or any other behavior used to contact, harass, track, or threaten someone. Online stalking includes spamming

[19] United Nations, A/RES/1566 (2004).
[20] Cybercrimes Act, Section 18(1).
[21] Ibid, S.22(3) (a)-(d).
[22] Ibid, S.33 (3)(a)-(d).
[23] Ibid, S. 23(5). See also Child's Rights Act, Section 277.
[24] Ibid, S.23(4) Cybercrimes Act.
[25] Ibid, S.23(1)(i).

(hacking) someone's email or social media account, threatening someone on the internet, using GPS or other software to monitor someone without their knowledge or consent, using spyware to track a person's computer activity. Section 24 of the Cybercrimes Act gives a 3-year jail term for convicts of cyber stalking while section 17 (1) of the VAAP Act outlines a 2-year jail term upon conviction.

6. Cyber bullying

Cyber bullying entails when a person intentionally and habitually causes emotional harm and discomfort to another by indulging in acts such as harassing, mistreating or making fun of another person's attributes online. All these could be done by phone calls, messages, or social media comments. Section 24(2) of the Cybercrimes Act criminalizes cyberbullying and gives a jail term between 5 to 10 years upon conviction.

7. Cyber Discrimination

Section 26 (1) (b) –(c) of the Cybercrimes Act makes it an offence for any person to threaten or insult others through a computer system or network due to differences in race, colour, descent, national or ethnic origin and religion. Discrimination is also prohibited by the Constitution[26] and can be enforced under a fundamental human rights action. It is also unlawful to use the internet to spread racial or xenophobic materials. This may be in form of jokes or comments that cause offense or hurt, name-calling or verbal abuse; harassment or intimidation, or public commentary that inflames hostility towards certain groups, tribe, religion etc[27].

8. Phishing

Phishing entails an act of making individuals disclose their personal or secret information. It is defined by section 58 of the Cybercrimes Act as :

the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through emails or instant messaging either in form of emails from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.

Section 32 (1) of the Act punishes the offense of phishing upon conviction for a jail term up to 3 years.

9. Spamming

Spamming is an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations. Section 32 (2) of the Cybercrimes Act punishes spamming and, upon conviction, a convict could be sentenced to 3 years imprisonment.

10. Fake News and Hate Speech

Fake news is defined as false news stories, often of a sensational nature, deliberately created to be widely shared or distributed for the purpose of generating revenue, or promoting or discrediting a public figure, political movement, company, etc. [28] Fake news despite being untrue stories are often spread as

[26] *Constitution of the Federal Republic of Nigeria* (CFRN) 1999, as amended, Section 42.
[27] Ibid, S.26 (2) of the Cybercrimes Act.
[28] *Dictionary.com.* www.dictionary.com/browse/fake-news. Accessed 5 October 2023.

propaganda on social media and it would interest you that most times due to their viral nature, they spread faster than wildfire. On the other hand, hate speech is a malicious speech made with vile and deliberately disseminated to provoke incitement, violence, hatred, strife and violence. The proponents of fake news do often intend to create an atmosphere of disinformation, confusion, fear, anger, and hysteria and ultimately confuse the end-receivers so that they would no longer be able to differentiate the truth from lies and then pollute their consciousness with hatred and vile against the object of attack. Constant consumption of fake news ensures consumers develop deep-set preconceived notions and opinions on people and events due to the deception they are fed with. According to Kalsnes,[29] there are three essential elements of fake news. They are format, falsity, and intention. It must be noted that while Kalsnes features are quite comprehensive, not all-fake news contains false information. Most of the time, fake news contains accurate yet misleading information.

There are various forms of fake news; the most common include the following

i. Satire or Parody[30]

In satire or parody, a message is deliberately crafted for amusement and fun, although without any intention to cause mayhem, depending on the circumstance, it may lead to harm, animosity or ill feelings against the subject of satire. Examples are parody characters who mimic important personalities or parody accounts on social media.

ii. False Connection[31]

False connection occurs when the headlines are intentionally crafted to attract attention of the public with oftentimes over bloated or exaggerated information with the assumption that viewers will simply read the headline and accept the falsehood. This is also known as click baiting.

iii. Misleading Content[32]

This occurs when a person deliberately takes a quote of an individual out of context and turns it to the headline often for mischief purposes. This is also called sound biting.

iv. False Context[33]

This occurs when the news is framed to make the truth come out as a lie in order to misinform the public on the true state of affairs.

v. Manipulated Content[34]

This is commonly known as “Photoshop” . It occurs when information is manipulated to deceive. This is common with pictures but advances in technology have created a new mode of manipulation for videos called “Deepfake”. Deepfake occurs when a computer algorithm is trained to recognize patterns in actual audio or visual recordings of a particular person, a process known as deep learning with the view to mimic the voice and face of an individual in a manner that cannot be distinguished from the

[29]Kalsnes, Bente. "Fake News." *Oxford Research Encyclopedia of Communication*, September 2018.
[30] Nwachukwu Obi, ‘’ Law and Fake News In Nigeria,’’ The Guardian, 26 Feb. 2019, http.www.https://guardian.ng/features/law-and-fake-news-in-nigeria/ Accessed on 15 Nov. 2023.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.

original. It thus can be used to devastating effect and has the potential to be the most dangerous form of Fake News.

vi. Fabricated Content[35]

Fabricated content as the name implies entails a deliberate authoring and circulation of false information with the aim of causing panic, harm and or unrest. Among the causes of fake news and hate speech include the inordinate selfish desire to be relevant and gain traffic, social inequality, greed for money and sometimes fake news is sponsored by government and State actors and the poor regulation of the internet.[36] It is pertinent to state that the right to freedom of speech and expression though guaranteed by section 39 (1) of the 1999 Constitution of the Federal Republic of Nigeria as amended, is not without limitations. In other words, the right to freedom of speech and expression does not exist in a vacuum. In the case of *Okedara v. Attorney General of the Federation*[37], the constitutionality of Section 24 (1) of the Cybercrimes Act was challenged on the ground that it contravenes the right to freedom of speech as enshrined in Section 39 of the Constitution. The Court held that Section 39 of the Constitution must be read with section 45 of the Constitution that stipulates the constitutional limitation to freedom of speech. Similarly, the Court of Appeal in suit number A/L/556/2017 in respect of the constitutionality of sections 24(1) and 38 of the Cybercrimes Act held that those provisions did not violate the human rights in question.

3.0 Conclusion

No doubt, misuse, and abuse of the internet robs the internet of its integrity and apart from its adverse socio-economic effects, it can lead to death of the victims and imprisonment of the abusers. The need then to have a safe, free, efficient, and reliable internet for all cannot be over emphasized. It is my recommendation that instead of the government and other stakeholders being reactive, waiting to gauge citizen's online rights to use the internet freely and even put offenders behind bars, the proactive approach of restoring the integrity of the internet should be adopted and vigorously pursued by orientation and mass civic education of citizens on how to use and be safe while surfing the internet. Just as every producer takes out time to prepare a user's guide and accompanies it with their products, so should the government and indeed every stakeholder protect the integrity of the internet by providing guidance on how this great innovation should be utilized for man's ultimate benefit. In addition, the Cybercrime (Prohibition, Prevention ETC) Act 2015 should be amended to reflect current realities in the digital world and lastly our security and enforcement agencies and their personnel should be adequately trained to respond appropriately in enforcing our laws relating to the use of the internet without compromising digital rights, in line with international best practices relating to the use of the internet.

[35] Ibid
[36] Samuel, A. O., et al. *Information and Knowledge Management Journal*, vol. 9, no. 2, 2019, ISSN 2224-5758 (Paper), ISSN 2224-896X (Online), DOI: 10.7176/IKM.
[37] CA/L/174/2018, Lagos Division.