COMMENTARY ON INADEQUACIES OF CYBERCRIME (PROHIBITION, PREVENTION, ETC) ACT 2015

Samson Ogana*

Abstract

Several jurisdictions have enacted laws regulating the conduct of persons on the internet. On the 5th of May 2015, the National Assembly enacted the Cybercrime (Prohibition, Prevention, etc) Act in Nigeria. This research examines the legal framework applicable to internet regulation in Nigeria in order to determine whether or not the framework is fit for purpose in the light of expected increase in the internet related crimes, in the future as a consequence of the popularity of the internet. This paper specifically examines Cybercrime (Prohibition, Prevention, etc) Act 2015, its benefits and inadequacies, its conflicts with other Acts of the National Assembly such as Evidence Act, Passport (Miscellaneous Provisions) Act, Central Bank of Nigeria Act, Banks and Other Financial Institutions Act (BOFIA), among others and the Constitution of the Federal Republic of Nigeria, 1999 as amended. Recommendations are made for a better regulation of cyberspace.

Introduction

Cybercrime has been defined as an 'umbrella term used to describe two closely linked, but distinct ranges of criminal activities'.[1] The two criminal activities have been referred to as cyber-dependant crimes, and cyber-enabled crimes.[2] The latter includes traditional crimes that are facilitated by the use of computers, computer networks or other types of ICT. Cyber enabled fraud falls into this category. The United Nations described cybercrimes as falling into the following five categories: (1) financial, (2) piracy, (3) hacking, (4) cyber-terrorism, and (5) online pornography.[3] Collectively, these types of crimes can constitute traditional crimes that are committed online, or they may amount to new crimes.[4] The primary objective of this research is to analyse the legal framework applicable to internet regulation and the need to assess the effectiveness of enforcement under the existing legal regime. The importance of examining this issue is evident from the impact that cyber related crimes are having in Nigeria and beyond.

Inadequacies of Cybercrimes (Prohibition, Prevention, etc) Act, 2015

After many years of concerted efforts[5], the Nigerian government finally enacted Cybercrimes (Prohibition, Prevention, Etc) Act, 2015. The Act is a landmark legislation representing the country's first foray into legislating on cyber security. The Act is commendable not only for the creation of certain specific offences[6], but also for an attempt to create institutions with

*[1] LLM, BL,LLB Liberal Studies Department, Federal Polytechnic Kaura Namoda Zamfara State, Nigeria

[1]The Crown Prosecution Service website: www.cps.gov.uk.

[2]HM Government, 'National Cyber Security Strategy 2016 – 2021', HM Government (2016).

[3]Ram Gopal, G Lawrence Sanders, Sudip Bahattacharjee, Manish Agrawal, and Suzanne Wagner, 'A Behavioral Model of Digital Music Piracy', *Journal of Organisational Computing and Electronic Commerce, 14 (2004), 89 – 105.*

[4]Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century (ABC-CLIO, USA, 2016), 57.

[5] The first attempt to enact such law was cybercrime bill 2005, followed by computer security bill 2008, cyber security bill 2011 and cybercrime act 2015

[6] Various offences are contain in Part III of the Act from Section 5 to Section 36 .

statutory power of investigation , prosecution[7] and the enforcement of cybercrime[8] in addition to the establishment of international legal co-operation to avoid dual criminality.[9] The Act's implementation could promote commercial activities, attract direct foreign investments and stimulate economic growth in Nigeria.

However, regardless of the massive applause which greeted the passage of the Act, it is equally necessary to highlight some of its flaws; this is in a bid to ensure the development of the law and to make it better. Some of the inadequacies of the Act include the following:

Infringement on Freedom of Expression

The right to comment freely on matters of public interest is one of the fundamental rights of free speech guaranteed under the 1999 Constitution of Federal Republic of Nigeria as amended. However, Section 24 of the Act seems to have infringed on the citizens' right to free speech. The section 24 deals with cyber stalking, it criminalizes the act of any person who sends to another through a computer network offensive materials by means of computer system or network. The Section provides:

> Any person who, knowingly or intentionally sends a message or other matter by means of computer systems or network that
>
> (a) Is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or
>
> (b) 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 shall 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

The government has abused this section of the Act by silencing opposing views in an online media by pressing charges against online journalists for expressing views that are considered unfavourable to the government, with security forces habitually arresting or intimidating online reporters.

The first known case decided under the Act is the case of *State v Oloketuyi* where a blogger was arraigned before the Federal High Court Lagos over alleged malicious publication against the Managing Director of Fidelity Bank Plc. The accused was alleged to have intentionally sent false message and other matters by means of computer network with the intent to cause annoyance, insult and ill-will to the complainant. He was eventually convicted under the section.

The dictatorial disposition of the Nigerian security agencies and the arbitrary interpretation of Section 24 of the Cybercrime Act by the government have led to public interest litigation by individuals[10] and civil society organizations. In Suit No. ECW/CCJ/APP/53/18 Laws and Rights Awareness Initiative, an NGO, approached the Community Court of Justice

[7] Ibid at Section 47
[8] See Section 41-43 of Cybercrime Act 2015
[9] Ibid at Section52
[10] See *Solomon Okedara v. Attorney General Of The Federation: FHC/L/CS/937/17*

(ECOWAS Court) on the unconstitutionality of Section 24 of the Nigerian Cybercrime Act and on the 10th day of July, 2020, the Court delivered judgment, and held that "such provision is not necessary in a democratic society and disproportionately violate the right to freedom of expression…" The Court further held that, "the provisions of Section 24 of the Cybercrime (Prohibition, Prevention etc) Act 2015 violates Article 9(2) of the African Charter on Human and Peoples Rights and Article 19(3) of the International Covenant on Civil and Political Rights".

Consequently, the Court ordered Nigerian government to repeal and amend Section 24 of the Cybercrime Act 2015 in accordance with its obligation under Article 1 of the African Charter and International Convention on Civil and Political Rights.

It is our anticipation that the federal government will comply with the order of the ECOWAS court, because ECOWAS court over years appears to be a toothless bulldog which can only bark without bite.

Conviction and dissolution of company

The Act creates a controversial provision where if a body corporate is charged and found guilty of an offence under the Act, the court may make an order for its winding up and the assets of the company will be forfeited to the Federal Government.[11] With respect, the provision is a bit heavy-handed and without recourse to the rights of creditors and shareholders who might be without the *mens rea*. In criminal jurisprudence, no one should be convicted of a crime without the mental element or guilty mind. It is not enough to convict, but the moral turpitude associated with a criminal conviction requires some element of fault. And to show that, *mens rea* is needed as held in *Sweet v Parsley*[12] that 'Parliament did not intend to make criminals of persons who were in no way blameworthy in what they did'. It is our view that there should be other more suitable punishment for a company than outright dissolution. This may even discourage investments.

Similarly, though the provision expands the provision Section 406 of the Companies and Allied Matters Act for compulsory winding up of a company, however, Section 29 of the Act seems to have put the cart before the horse when it provides that such body corporate will not be liable if it can prove that it had no knowledge of the offence and that due diligence was exercised to prevent the commission of the offence. The burden of prove in criminal offences is always on the prosecution, however this section places the burden of proving the offender's innocence on him. This offends against the laid down principle of burden of proof under Nigerian criminal justice system.

Interception of personal data

The Act equally provides that under certain circumstances, a Judge may order service providers to 'intercept, collect, record, permit or assist competent authorities with the collection or recording of content data and or traffic data.[13] The Act defined content data as the actual information or message sent across during a communication session.[14]Traffic data means any computer data relating to a communication by means of a computer system or network, generated by a computer system that formed a part in the chain of communication, indicating the

[11] Ibid at section 29(b)
[12](1970)AC 132
[13] Ibid at Section 39(a)
[14] See Section 57 of the Act

communication's origin, destination, route, time, date, size, duration, or type of underlying service.

It is our opinion that content and traffic data are synonymous with European Union idea of personal data which is defined as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental economic, cultural or social identity of that natural person[15].

In Nigeria, it is contrary to the constitutional provision to intercept individual personal data. Section 37 of the 1999 Constitution, as amended, provides that 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected.' For anything to even attempt to derogate from this constitutional right should be a serious crime. Unfortunately, the Cybercrime Act does not qualify the type of alleged crimes that can trigger a request for interception of communication; the reality is that the request can be made for an offence that is a 'minor offence'.

Cancellation of International passport

Similarly, the Cybercrime Act states that any individual who is convicted of an offence under the Act *'*shall have his International passport cancelled[16]*'*. This would appear to be a violation of the constitutional right of freedom of movement of Nigerians as laid out in Section 41 of the 1999 constitution, and as decided in the case of *Director of SSS v Agbakogba*.[17] In this suit, Olisa Agbakoba, was invited by the Netherlands Organization for International Development and Cooperation (NOVIB) to attend a conference which was scheduled to take place between 22nd and 25th April, 1992. On 21st April, 1992, he went to Murtala Muhammed International Airport, at Ikeja Lagos with a view to traveling to The Hague in the Netherlands. However, he could not board the plane because he was stopped by officers of the Nigerian State Security Service (SSS) who impounded his passport without giving any reason for the seizure. After fruitless efforts to regain the passport, the Applicant instituted a suit under the Fundamental Rights (Enforcement Procedure) Rules seeking inter alia:

> A declaration that the forceful seizure of the applicant's passport by agents of the State Security Services is a gross violation of the applicant's right to personal liberty, freedom of thought, freedom of expression and freedom of movement respectively guaranteed under Sections 32, 35, 36 and 38 of the Constitution of the Federal Republic of Nigeria 1979, and is accordingly unconstitutional and illegal. An order of mandatory injunction directing the respondents to release applicant's passport forthwith.

The court granted the Applicant's prayers and ordered for the release of his passport.

From the analysis of the entire judgment in Agbakoba's case, it can safely be concluded that the case would be a good authority for the fact that the right to travel outside Nigeria is constitutionally protected. Further, the Passport (Miscellaneous Provisions) Act[18] envisaged the cancellation of a passport only in cases where "the passport is obtained by fraud, the passport has

[15] Article 4 General Data Protection Regulation 2018
[16] Ibid at Section 48
[17] (1999) 3 NWLR (Pt. 599)
[18] See section 5(1) of the Act

expired, a person unlawfully holds more than one passport at the same time, or it is in the public interest so to do". In the case of the Cybercrime Act, any cancellation of a passport under the basis of the conviction of an offence would have to be justified as 'in the public interest'. Since all offences under the Act could presumably lead to a cancellation of a passport, the absurdity would be that a minor offence like 'cyber-squatting' would lead to the individual having his/her passport cancelled. This provision is potentially unconstitutional.

Criminal Obligation for Financial Institutions

Apart from the flaws discussed above, the Act equally creates several duties for financial institutions[19] and service providers,[20] even when many of the duties created duplicate measures already imposed by industry specific regulators[21]. The burden of these duties is compounded by the criminal liability imposed for failure to meet them[22]. The view has been expressed that this may lead to chaotic compliance with the Act[23]. This provision also stretches the regulatory powers of the Act to the operations of Banks and Financial Institutions whose operations are already governed by other laws[24]. This creates an overlap in the applicability of the Acts. Sections 55 and 56 of Banks and Other Financial Institutions Act (BOFIA) provide that where the provisions of the Companies and Allied Matters Act or Nigeria Deposit Insurance Corporation Act are inconsistent with the provisions of the BOFIA, the provisions of the BOFIA shall prevail. It is our view that the same provisions should be applicable in case of the Cybercrime (Prohibition, Prevention etc) Act 2015, conflicts with the BOFIA Act.

Enforceability of Cybercrime Act 2015

The Cybercrime Act mandates "all relevant law enforcement agencies" to enforce it[25]. As the case is, the tradition in Nigeria criminal justice administration system is to enact a law, which prohibits certain actions as crime and create an institution to enforce those specific laws.[26] The tradition was not only broken with the Cybercrime Act, but the law ended up creating too many "cooks" in the law enforcement agencies resulting in a situation where no one could actually enforce the Cybercrime Act[27]. The side effect of this lacuna is that it appears Nigeria currently does not seem to have anyone taking up the leadership of enforcing the Cybercrime Act, because no agency will truly see it as its responsibility.

The administration of evidence

Some of the provisions of the Cybercrime 2015 Act are inconsistent with the provisions of the Evidence Act 2011.

(a) With regards to admissibility of evidence obtained from foreign countries, Section 53 of the

[19] See section 37 of Cybercrime Act 2015

[20] Ibid at section 38

[21] E.g the CBN Guidelines on eBanking and Card Issuance and Usage Guidelines. by virtue of these guidelines, banks are responsible for the security of the payment cards they issue; and are liable to reverse electronic transactions reported by card holders to have been executed fraudulently, and chargeback

[22] See section 37(3)

[23] Basil U.:Cybercrime Act does not create an enforcement agency. Available on www.thisdaylive.com

[24] The Central Bank of Nigeria Act and the Banks and Other Financial Institutions Act (BOFIA)

[25] Section 47 Cybercrime Act 2015

[26] This is why there is NAFDAC enforcing pharmaceutical related law and NDLEA responsible for the narcotic related. The EFCC is responsible for economic crimes and the Copyright Commission is only conferred with the authority to enforce copyright laws

[27] Ibid at note

Act provides that evidence obtained in a foreign country can be used in court proceedings in Nigeria if such evidence is authenticated by a judge, magistrate or Justice of Peace, or by the seal of a ministry or department of the Government of a foreign state. This is contrary to Section 106(h) of the Evidence Act which provides that foreign evidence can be used in Nigeria where it is a copy and it is sealed by a foreign or other court to which the original document belongs or be signed by a Judge, it can be certified by a notary public or a consul or diplomatic agent and shall be admitted upon proof of the character of the document according to the Law of the foreign country. The Section of the Evidence Act is more elaborate on persons who can certify foreign evidence from those provided under the Cybercrime Act.

(b) With respect to admissibility of electronic signature, Section 93(2) of the Evidence Act permits the use of electronic signature for any form of document while Section 17(2) of the Cybercrime Act removes certain documents from the purview of electronic signature. Section 17(2) of the Act removes the following from the categories of documents which would not be valid by virtue of an electronic signature. They include; creation and execution of wills, codicils and or other testamentary documents, death certificate, birth certificate, matters of family law such as marriage, divorce, adoption or related matters, issuance of court orders, notices, official court documents, etc. This Section is inconsistent with Section 93(2) of the Evidence Act which provides: "Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences".

The inconsistency could create problems of enforcement of such document in court, while the party seeking for it to be admitted in evidence will rely on the Evidence Act which permits electronic signature for every form of document. The party that wants it expunged would rely upon the Section 17(2) of the Cybercrime Act which limits the applicability of electronic signature to certain documents.

The question that then arises is which Act will take precedence over the other in case of inconsistency since both are Acts of National Assembly and none is superior to the other? In *Federal Republic of Nigeria v. Osahon*[28], the Supreme Court held that where there are two conflicting Acts of the National Assembly, the provisions of the specific would override the general provisions but where there is a constitutional provision on that point the provisions of the constitution shall govern the interpretation. The rule laid down by the Supreme Court would not, in our view apply in the conflict between the provisions of the Evidence Act and the Cybercrime Act, as both Acts can be considered as specific Acts. The issues governing electronic signature is not provided for in the constitution. This will be a subject of litigation in the courts and the court would be left to decide which Act will prevail.

With respect to the provision of the Constitution and the Act, the provisions of the Constitution take precedence over any law enacted by the National Assembly even though the National Assembly has the power to amend the Constitution itself. Section 1(1) and 1(3) of the Constitution of the Federal Republic of Nigeria state that, Section 1(1) "This Constitution is supreme and its provisions shall have binding force on all authorities and persons throughout the Federal Republic of Nigeria." Section 1(3) "If any law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall to the extent of the inconsistency be void." The courts in their numerous decisions on the supremacy of the

[28] (2006) 5 NWLR pt 973

Constitution have interpreted the foregoing sections to mean that the legislative power of the legislature cannot be exercised inconsistently with the Constitution[29]. Where it is so exercised it is invalid to the extent of such inconsistency. Where the Constitution sets the condition for doing a thing, no legislation of the National Assembly can alter those conditions in any way directly or indirectly. Therefore, provisions relating to infringement on freedom of speech ought to be expunged forthwith for its inconsistency with the provision of the Constitution

Recommendations

The Act is commendable for its salient provisions on the regulation of internet and other related matters. However, there are still some pitfalls, loopholes and inadequacies. This call for the following recommendations:

- Although the Act imposes a duty on the office of the National Security Adviser to be in charge of the enforcement of the provisions of the Act, no specific agency is saddled with responsibility of enforcing it;
- Therefore, there should be clarity as to the law enforcement agencies that are in charge of the enforcement of the provisions of the Act.
- We recommend that a cybercrime agency should be created and should be well trained for the task of enforcement.
- There is need for Nigeria to become a signatory to the Budapest Convention on Cybercrime in order to enhance its international cooperation in combating cybercrimes. Though Budapest Convention is a regional instrument, but it remains the instrument with the broadest reach on cybercrimes presently which had been ratified by over 40 countries including the US and some countries outside Europe since it was drafted by the Council of Europe in 2001,
- The Cybercrime (Prohibition, Prevention, etc) Act 2015 should be amended without delay to ensure that those sections that conflict with the Constitution and other Acts of the National Assembly are expunged.
- 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.
- The high handedness of government officials is needless. There is the need for executive to live above board to the point where they do not necessarily see criticisms as attacks on their personalities, rather, as public probity.

Conclusion

Apart from making necessary amendments as recommended, it is pertinent to note that the Act alone cannot solve the many problems associated with internet regulation in Nigeria. The National Assembly should be able to enact more legislation to combat different aspects of cyberspace, including issues relating to cloud computing, data protection, smart contracting, artificial intelligence, crypto currency and other sundry issues.

[29] *INEC v. Musa* (2003) FWLR (Pt. 145) 729, *Att.-Gen., Abia State v. Att.-Gen. Federation* (No. 2) (2002) FWLR (Pt. 101) 1419, *Att.-Gen., Abia State v. Att.-Gen. Federation* (2003) FWLR