NIGERIA'S CYBERCRIME (PROHIBITION, PREVENTION, ETC) ACT 2015 AT EIGHT: CLASS ACT OR THE NEW NORMAL?

Abstract

The Cybercrime (Prohibition Prevention Etc) Act (CPPA) 2015 is the law that governs the activities in Nigerian cyberspace. Since its inception, cybercrime has rapidly been on the increase in Nigeria. It has faced many hurdles especially calls regarding to its repeal. Literature calling for the repeal of the CPPA abounds in newspapers articles, online website et al, the reasons being given regarding its repeal range from its constitutionality of the act, other reasons include fundamental human rights breaches of the Act. Adopting a doctrinal approach the article argues that the constitutionality of the Act, fundamental human right breaches challenges is only a fragment of the inefficacy of the Act. By examining the provisions of the Act, the article unearths other deficiencies hitherto not highlighted, namely, inelegant drafting, lack of clarity, and onerous and punitive nature of the Act. Based on this, the article therefore lends credence to the argument for its amendment.

Keywords: Cybersecurity, Cyber-legislation, Internet, CPPA 2015

1. Introduction

The Cybercrimes (Prohibition, Prevention, Etc) Act (CPPA) was signed into law on May 15, 2015. Currently it is the major law used to combat cybercrime in Nigeria. On its eighth anniversary, it is pertinent to look at it with fresh lens. This article examines this all importance piece of legislation as it plays its legislative role in the curbing of cyber criminality on the web. Global cybercrime is on the increase especially in the post Covid-19 era; a fit for purpose legislation is essential to deter miscreants on the web. Statistics have shown that roughly 5.7 billion people use the internet every day;[1] there is estimation that there will be more than 7.5 billion internet users in 2030.With this increased internet usage and broad band penetration, new types of cyber criminality crop up on the internet constantly. This trend shows no signs of slowing, as sophisticated tools and methods become more widely available to threat actors at relatively low (or in some cases no) cost.[2] Technology has so much evolved on the internet; fraudulent activities on the web now range from hacking, phreaking, Trojan horses to Ransom ware. These cyber threats are so destructive and grave to put human lives in danger even poses risks to life of citizens.[3] In 2017 A cyber-attack that affected more than 60 trusts within the United Kingdom's National Health Service (NHS) spread to more than 200 000 computer systems in 150 countries,[4] Many hospitals in the UK could not access patient records, which led to delays of surgeries and cancelled patient appointments.

More recently Artificial intelligence, deep fake technology, machine learning, robotics, quantum computing are the current trends in cybercrime.[5] Recently a photo of Pope Francis wearing Balenciaga jacket went mega-viral on the internet. But there was just one problem: The image was not real but misinformation case. It was created by Pablo Xavier, a 31-year-old construction worker from the Chicago using the Artificial intelligence art tool Midjourney.[6] These Artificial intelligence tools are used by hackers for advanced attacks making their assaults more complex and challenging to detect. [7] With the adoption of e elections and use of the cyberspace for many critical functions, the global economy is at a precipice in the hands of cybercriminals. With these complex and unprecedented incident on the worldwide web, the CPPAs role as the sole regulation on the Nigerian cyberspace is called to account. This article is divided into five parts, Part II, immediately following the introduction we will provide a brief account of Nigeria's challenges with cybercrime. We will show that these challenges negatively affect Nigeria's reputational and economically as foreign direct investment is stalled by this cyber-insecurity. In Part III, we will recount the history of the CPPA, and show that cybercrime is a radically different crime and complex as well. We highlight how prior to the enactment of the CPPA, cybercriminals were charged with lesser

***By Obinne C. OBIEFUNA, LLB, LLM (Essex), PhD (Nig.),** Lecturer, Department of International and Comparative Law, Faculty of Law, University of Nigeria, Nsukka. Email:obinneobiefuna@gmail.com,

***Emeka ADIBE, LLB, LLM (Ottawa), PhD (Nig.),** Lecturer, Department of Jurisprudence and Legal Theory University of Nigeria, Nsukka; and

***Adrian OSUAGWU, LLB (Nig.), LLM (Nig.), PhD (in view),** Lecturer, Department of International and Comparative Law, Faculty of Law, University of Nigeria, Nsukka.

[1] Jason Wise, How Many People Use The Internet Daily In 2023 April 10 2023< https://earthweb.com/how-many-people-use-the-internet-daily/> accessed 7th May 2023

[2] above

[3] A B Hassan, F D Lass , J Makinde Cybercrime in Nigeria: Causes, Effects and the Way Out, [2012] *ARPN Journal of Science and Technology,* 2(7), 626 – 631

[4] Roger Collier, NHS Ransomware Attack Spreads Worldwide, [2017] *Cantina Medical Association Journal CMAJ* 189(22)

[5] Kayleen Devlin ,Joshua Cheetha, Fake Trump Arrest Photos: How to spot an AI-generated image, March 24 2023 , <https://www.bbc.com/news/world-us-canada-65069316> accessed 7th May 2023

[6] Chris Stokel-Walker, We Spoke To The Guy Who Created The Viral AI Image Of The Pope That Fooled The World <https://www.buzzfeednews.com/article/chrisstokelwalker/pope-puffy-jacket-ai-midjourney-image-creator-interview> accessed 7th May 2023

[7] Chuck Brooks, Cybersecurity Trends & Statistics For 2023; What You Need To Know, March 5 2023 <https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=2ca1ad5f19db> accessed 7th May 2023

offences found in the statute books giving room for them to escape punishment in cyber-related offences. This was plausible because of the lacuna in existing laws. In Part IV we critically assess CPPA to gauge its fitness for purpose in terms of deterrence of cybercrime. Specifically its provisions are scrutinized to weigh its clarity of language, precision effectiveness and accessibility.[8] This is followed by concluding remarks.

2. **Nigeria's Cyber Criminality Challenge**

The world of cybercrime is sophisticated and transnational, spanning across multiple jurisdictions.[9] It has become a coordinated cartel infrastructure involving actors across the world.[10] advancement in information and communication technology (ICT) has created room for the emergence of cybercrime. Access to computers, the internet and security vulnerabilities in cyberspace have made the perpetration of cyber-related crimes more pervasive.[11] The advent of mobile phones and other computer devices in Nigeria and the provision of internet services by accredited Global System for Mobile Communication (GSM) providers has endeared the internet to many Nigerians.[12] Cybercrimes recorded a massive rise in the first six months of 2022, with the global yearly cost of cybercrime reaching $6 trillion at the end of 2021.

Nigeria has a chequered history with cybercrime. Nigeria is often cited as a breeding ground for the most nefarious practices on the web because of the activities of some of her citizens. The country is ranked third in global internet crime while 7.5 per cent of the world's hackers are said to be Nigerians.[13] Internet scams perpetrated by Nigerians hit a 174 per cent mark.[14] Economically Nigeria loses about N127 billion yearly to internet fraud, an amount which represents 0.08% `of Nigeria's gross domestic product.[15] Certainly, a nation with such a high incidence of crime cannot grow or develop for crime is the direct opposite of development.[16]

Examples abound as to the enormity of finances carted away by Nigerian cybercriminals .In 2021 Salau Femi hacked into the System of a First-Generation Bank and made away with One Billion, Eight Hundred million Naira.[17] The high proliferation of cybercrime in Nigeria is the consequence of youth population and Information technology know how. It is estimated that 60 per cent of Nigeria's population is under the age of 25, [18] these youths are mostly unemployed or underemployed. Furthermore one consequence of the introduction of the cashless policy in Nigeria is increased proliferation of cybercrime. The digital revolution of e-banking has resulted to an equivalent revolution in e-banking frauds. The Nigeria Inter-Bank Settlement System (NIBSS) reported that the first nine months in 2020, Nigerian banks lost over N5bn to fraud related to electronic transfers. In five years alone a particular new generation bank lost N871m to scammers and hackers. It's no rocket science that e banking payment system has encouraged the increase of cybercrime in Nigeria. Rising up to the occasion, Nigeria's anti-graft agency, EFCC, convicted 2,847 persons of cybercrime across the country as of October 2022. The EFCC chairman, Abdulrasheed Bawa, disclosed this when he appeared before the Senate Committee on Anti-Corruption. In 2021, the EFCC announced the total number of cybercrime convictions was e 2,220 – the highest since its inception.[19] These incidents have continued to have negative effects on the image of Nigerians across the globe, as they are always perceived as fraudsters. They have also affected international recognition of the country's young entrepreneurs, and the granting of visas to those with legitimate business interests in the US and other parts of the world.[20]

---

[8] Tom Bingham, *The Rule of Law* (London, Allen Lane, 2010) 7

[9] Ikenga K.E. Oraegbunam, 'Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses' [2016] *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 7, 26-40.

[10] Uche Igwe Nigeria's Growing Cybercrime Threat Needs Urgent Government Action,9 June 2021<https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/ > accessed 7th May 2023

[11] Ikenga K.E. Oraegbunam & Kenneth U. Eze, 'The Internet and its Facility for Criminality: Some Unique Difficulties for Investigation and Prosecution',[2014] *Nnamdi Azikiwe University Journal of International Law and Jurisprudence,* (5)12-26.

[12] Akeem Olalekan Ayub ,Linus Akor, Trends, Patterns and Consequences of Cybercrime in Nigeria [2022] *Gusau International Journal of Management and Social Sciences* (5) (1) 241

[13] This Day Newspapers , The Challenge Of Cybercrime <https://www.thisdaylive.com/index.php/2022/12/23/>ybercrimes/ accessed 7th May 2023

[14] Business Day, Nigeria recorded a 174 % increase in cybercrime in six months 18 November 2022 <https://businessday.ng/news/article/nigeria-recorded-a-174-increase-in-cybercrimes-in-six-months-heres-why-you-should-be-bothered/> accessed February 5 2023

[15]Sony Aragba-Akpore, Digital Literacy And Rising Cybercrimes
< https://www.thisdaylive.com/index.php/2022/06/01/digital-literacy-and-rising-cyber-crimes/ >accessed February 5 2023

[16] Adedeji Oyenuga, Lucrative and Hidden: Factors Influencing Cybercrime Involvement among Youth in Metropolitan Lagos[2019]*International Journal of Social Sciences and Humanities Reviews* (9)(2); 238

[17] https://www.specialfraudunit.org.ng/en/?p=1186 accessed February 5 2023

[18] How Nigeria's Expanding Youth Population Fuels Retail Growth in Nigeria
<https://www.thisdaylive.com/index.php/2023/02/23/how-nigerias-expanding-youth-population-fuels-retail-growth-in-nigeria/> accessed February 5 2023

[19] Queen Esther Iroanusi, Over 2,800 Persons Convicted of Cybercrime in 2022 – EFCC October 27 2022 <https://www.premiumtimesng.com/news/top-news/562065-over-2800-persons-convicted-of-cybercrime-in-2022-efcc.html> accessed February 5 2023

[20] N 15 above

Currently a new development has emerged in the cybercrime underworld. Cybercrime 'training schools' are springing up all over Nigeria.[21] Youths are enrolled in these so called school and for a fee they are taught various aspects of cyber scam e.g. phishing, breaking encryptions, online fraud , hacking romance scam etc. Law enforcement agents have recorded numerous arrests concerning this. In Abuja an owner of the internet scam academy was arrested alongside 16 of his trainees aged between 16 and 27 years.[22] The Abuja arrest was similar to an earlier one in Eket, Akwa Ibom State where 23 suspects including operators and trainees were nabbed by officials of the EFCC. The suspects were between the ages of 19 and 35 years. They were undergoing training in various aspects of the internet scams such as love scam, online trading scam. But the biggest breakthrough was the arrest of 402 suspects in the Lekki, Ajah axis of Lagos State between April and June 2021. It is obvious that urgent measures should be in place to quell this dangerous precedent especially as the country begin to adopt full digital economy, it is important that Nigeria build resilience against these threats to ensure trust in the system.[23] With this record cyber-misbehaviour by Nigerians The CPPA 2015 seem to have failed in its function to regulate the Nigerian cyberspace. There have been calls for its repeal.[24] A cybercrime statute, which provides efficient and effective legal backing for investigating, prosecuting, and curtailing electronic invasions and unlawful conducts, is urgent and necessary.[25]

3. History of the CPPA 2015

The Cybercrime (Prohibition Prevention, Etc) Act 2015 is a landmark legislation, representing the country's first foray into legislating on cyber security. Prior to its enactment cybercrime cases were tried under various legislations.[26] The CPPA was also enacted in order to avert the situation in *R v Gold*[27], a British case where the defendants were acquitted because there were no laws to prevent unlawful access to a computer. The Cybercrime (Prohibition Prevention, Etc) Act 2015 is a federal law enacted to check the excesses of Nigerians on the World Wide Web. Nigeria experienced tremendous growth in telecommunications usage and internet penetration because of the proliferation of Internet Service Providers (ISPs) and Cybercafés. Consequently, fraudsters migrated to the internet to perpetrate crimes on cyberspace. International and domestic reports adjudged Nigeria as major global hub of cyber-criminal activity, being one of the countries with the highest rates of cybercrime perpetration in the world.[28] With severe negative implications for national economic development, national security, international relations and also human rights and human security,[29] Nigeria faced a lot of international pressure from western countries whose citizens were being defrauded by Nigerians on cyberspace to promulgate a cyber specific law. In *FRN v. Nwude &ors*[30] the defendant and his accomplices impersonating former CBN Governor Paul Ogwuma and other top officials of the Ministry of aviation defrauded a Brazilian citizen Nelson Sakaguchi of 190 Million USD. Countries like United States, Britain and even the EU had citizens affected by the online activities of Nigerians. The law was enacted based on the understanding that threats to information and communication technology are a danger to Nigeria's reputation, national security, economic, political, and social fabric. The Act also sought to ensure the protection of critical national information infrastructure, the protection of computer systems and networks, electronic communications, data and computer programmes, intellectual property and privacy right. It gives effect to the 2011 ECOWAS Directive on fighting cybercrime. With the deregulation of the telecommunications sector at the turn of the century, and the increased ICT adoption in Nigeria, the world became a global village. The advancement of the Internet in recent years saw many criminal elements in this country use modern network infrastructure, such as the Internet and mobile phones to commit crime. A new spate of crime, cybercrime became synonymous with Nigeria; Computer-related forgery, computer-related fraud, and other computer-enabled financial crimes blew up on Nigerian cyberspace. These crimes affected mainly foreign expatriates. The onus was on Nigeria to provide an effective, unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of this emerging crime.

[21]EFCC arrests proprietor of yahoo yahoo school in Benin December 16 2022 https://www.thecable.ng/efcc-arrests-proprietor-students-of-yahoo-yahoo-school-in-benin accessed February 5 2023

[22]Ishola Oludare yahoo yahoo training school discovered in Abuja February 18 2021 https://dailypost.ng/2021/02/18/yahoo-yahoo-training-school-discovered-in-abuja/ accessed February 5 2023

[23] NITDA to collaborate with Nigeria police on NPDR Enforcement https://nitda.gov.ng/nitda-to-collaborate-with-nigeria-police-on-npdr-enforcement/4951/ accessed February 5 2023

[24] See F.Tarpael 'Senate Seeks Review of Nigeria's Cybercrime Act.'(3rd November 2017), available at https://guardian.ng/business-services/senate-committee-seeks-review-of-nigerias-cybercrime-act/ accessed 7th March 2023.

[25] Ikenga K.E. Oraegbunam, 'The Nigerian Police and Problems of Cybercrime Investigation: Need for Adequate Training', [2015] *The Nigerian Law Journal*, (18) (1), 1-28

[26] *Mike Amadi v. Federal Republic of Nigeria*6 (2008) 12 SC (Pt. III) 55.

[27] (1988) AC 1063.

[28] NCC Report, effects of cybercrime on foreign direct investment and national development https://ncc.gov.ng/docman-main/industry-statistics/policies-reports/735-nmis-effects-cybercrime-foreign-direct-investment/file accessed 24April 2023

[29] FE Eboibi, A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015, [2017] *Computer Law & Security Review* 33(5) 19

[30] [2016] 2 EFCCLR 149 at 161.

Prior to the enactment of the Act, there are laws in existence that accommodate situation interpreted to incorporate cybercrimes and fill some need regardless of how restricted.[31] These laws include: Nigerian Criminal Code Act, Penal Code Act, Economic and Financial Crimes Commission (Establishment) Act, and Advanced Fee Fraud and other Related Offences Act. The Economic and Financial Crimes Commission Act (Amendment) Bill 2010 Nigerian Evidence Act 2011[32] In *Amadi v. Federal Republic of Nigeria*,[33] a case involving the cybercrime of phishing was decided based on the Advance Fee Fraud Act. The accused Amadi, cloned the official website of the Nigerian Economic and Financial Crimes Commission, which he used to defraud several persons. Amadi was later arrested over fraud amounting to the sum of US$125, 000.00. He was sentenced to ten years in jail. His appeals to the Court of Appeal and Supreme Court were all dismissed and the ten year jail term was reaffirmed. He was convicted based on the crime of fraud i.e. he collected money from the victims of his crime, and not on the basis that he cloned the website of the EFCC. He was not charged for the crime of phishing for it was unknown under the Advance Fee Fraud and Other Related Offences Act. Indeed the Criminal code, the Penal code and other penal legations in Nigeria pre 2015 had identifiable gaps in prosecuting cyber offences. In the case of *FRN v. Ikonji & anor*[34] the defendants were each sentenced to 45 years imprisonment for impersonating the former executive chairman of EFCC, Mallam Nuhu Ribadu to dupe one Mr. William Ellison, an American, of the sum of US$750, 000. They were tried and convicted for identity fraud and not the cybercrime of phishing. Again due to the non existence of a cybercrime specific law, the charge of phishing was not preferred against them.

In the case of *FRN v. Odiawa*,[35] the defendant was arraigned before the High Court of Lagos State, Ikeja Judicial Division on 10th January, 2005 on information containing 58 count charges to which he pleaded not guilty. None of the 58 counts contained a cybercrime specific offence; as there was no cyber legislation in Nigeria as at the time this case was instituted. Accused defrauded an American citizen Robert Blick of 20.5 million dollars on the pretext of getting him a contract. The 58 counts of offences alleged against the accused fell into four broad categories namely conspiracy to obtain by false pretence, obtaining by false pretence, forgery, Uttering and Possession of documents containing false pretences contrary to the Advanced Fee Fraud and Other related Offences Act, Cap. A6, Laws of the Federation of Nigeria, 2004. In the course of the trial, amendments were made because the prosecutor was trying to grapple with the nature of crime committed by the accused hence it was committed with the aid of computers and there was no cybercrime specific law in Nigeria. The accused was convicted only because there were hardcopies of computer generated documents. The conviction may not have held if only soft copies of computer generated documents were used by the accused in carrying out the crime.[36] The defendant was found guilty and sentenced accordingly. These cases were successfully tried due to the little complexity involved in their commission and the fact that the cybercrime element was jettisoned by the prosecutors. With the outcome of these cases, it became imperative that a cyber specific legislation is paramount. Efforts were intensified by the National Assembly to pass a cybercrime Act. Four private member bills were introduced at both chambers of the National Assembly seeking to provide a legal framework to combat cybercrime and other related offences. These include the Computer Security and Critical Information Infrastructure Protection Bill 2005; Cyber Security and Data Protection Agency Bill 2008; Electronic Fraud Prohibition Bill 2008; Computer Misuse Bill 2009 Nigeria Computer Security and Protection Agency Bill 2009.[37] Finally on May 15 2015, the Cybercrime Prohibition Prevention Act was assented to by the then president Goodluck Jonathan and became the country's cybercrime legislation.

4. CPPA as a Cyber Regulatory Act

It was a long process to the enactment of the CPPA, 2015 and until the Act is reviewed, it is the only legal instrument with which the government will fight the menace of cybercrime and the only tool for Judges to bring cybercriminals to justice. It is therefore important to review the strengths and weaknesses of the provisions of the Act. An attempt is made to address some sections of major concern below. The Act is structured into 8 parts, 59 sections and a schedule as follows: Part 1 Provides for the Objective and application of the Act. S. 1(1) states that the objective is to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The provision in Section 1(b) shows that the intention of the Act is to ensures the protection of critical national information infrastructure while section 1(c) clearly declare that the Act will promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs intellectual property and privacy rights. The application of the Act is provided for in section 2, and it states that the provision of the Act shall apply throughout the Part 2, Provides for protection of critical national information infrastructure and designate certain computer systems or networks as critical national information infrastructure and also provide for audit and inspection of critical national information infrastructure.

[31]Bello Adesina Temitayo, Anatomy of Cybercrime in Nigeria; The Legal Chronicle <https://Papers.Ssrn.Com/Sol3/Papers.Cfm?Abstract_Id=3055743> accessed 24th January 2023.

[32] A Rotimi, 'Rep Passes Anti-Cybercrime Bill for Second Reading', *Daily Independent*, Nov. 27, 2012.

[33] Unreported judgement of the Nigerian Federal Court of Appeal (Lagos Judicial Division), Appeal Case No: CA/L/389/2005.

[34] Unreported J. Francis., 'American loses N97 million to fake EFCC chairman' (10 March, 2005) < http://nm.lohttpssss15 > accessed 24th January 2023.

[35] (2008) ALL FWLR (Pt. 439) 436.

[36] *See Abdul v. FRN*. (2007) 5 EFCLR 24. Here the trial judge did not appreciate that a soft copy of a document could be said to still be possession of accused. He thus discharged and acquitted the accused who was charged for fraud.

[37] A Rotimi, 'Rep Passes Anti-Cybercrime Bill for Second Reading', *Daily Independent*, (Lagos, ***Nov. 27, 2012***.)26

Offences and penalties are provided for in part 3. This part covers a wide range of offences which include unlawful access to computer, registration of cyber café', unlawful interception, computer related forgery, cyber terrorism, identity theft and impersonation, child pornography and related offences, breach of confidence by service providers and many more. This part also provides for the punishment for all the offences. The duty of financial institutions is covered in part 4. In this part, section 37(1)(a) states thus:

> A financial institution shall
> (a) 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 ….
> (b) Apply the principle of know your customer in documentation of customers …. Except for electronic specific, this election of the Act is impart-material with section 5(1) (2)(a)(b)(3)(4)(5)(6) and (7) of the money laundering Act, 2011

Part 5 which provides for administration and enforcement of the Act and covers Co-ordination and enforcement, establishment of cybercrime advisory council, functions and powers of the council and establishment of national cyber security fund. Part 6 provides for arrest, search, seizure and prosecution. It specifically mentioned power of arrest, search and seizure, obstruction and refusal to release information, prosecution of offences, order of forfeiture of assets and order for payment of compensation or restitution. Section 50(1) provides thus:

> The Federal High Court Located in any of Nigeria, regardless of the location where the offence is committed, shall have jurisdiction to try offences under this Act, if committed under this part, the provision for international cooperation include: extradition, request for mutual assistance, evidence pursuant to a request, form of request from a foreign state, expedited preservation of computer data and designation of contact point.

Part 7 provides for Jurisdiction, extradition and International Co-Operation. The federal high court was mandated with the jurisdiction to try cyber offenses. This part provides that the Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. Part 8 provides for regulations, interpretation of key terms and citation. Terms used in the Act are defined in this part to give true meaning to the words in context of the Act.

Section 5 to Section 36 of the Cybercrime Act, contains offences punishable under the Act and penalties in respect of the offences. Section 5 of the Act prescribes the punishment for a person who commits an offence contrary to the critical national information infrastructure. Such person would be liable under to 10 years imprisonment. If the act causes bodily harm to any person, the punishment is 15 years imprisonment; if the act causes death to another, the penalty is life imprisonment.

Section 6 of the Act criminalizes unlawful access to a computer. Section 6(1) provides that any person who without authorization, intentionally accesses in whole or in part a computer system or network for fraudulent purposes and obtain data that are vital to national security commits an offence and would be liable to five years imprisonment or fine not less than N5,000,000 or both. If the person has intent to obtain computer data, the punishment is seven years.

5. The Nature of the Act: Deterrence, Vagueness, Punitive and Onerous

Deterrence

The CPPA does not live up to the gold standard in efficacy of laws.[38] In criminal justice system, one of the purposes of criminal legislations is to act as deterrence.[39] Deterrence is the use of punishment to prevent the offender from repeating his offense and to demonstrate to other potential offenders what will happen to them if they follow the wrongdoer's example.[40]In deterrence, the CPPA has performed abysmally. Most of the sentencing sections prescribed light sentences. Besides life imprisonment for attacking critical infrastructure,[41] the average sentence for committing cybercrime stipulated in the CPPA is seven years.[42] Hacking criminalized under S 14 of CPPA which is prevalent in Nigeria carries a paltry sentence of 3-7 years. Likewise the monetary fine is incredibly low;[43] for example s 33 of the Act which criminalises spreading of computer virus has a fine penalty fixed at one million naira. In committing cybercrime, Cybercriminals obtain huge financial benefit. In 2021 Salau Femi hacked into the System of a First-Generation Bank and made away with One

[38] Ss5 -36 of the CPPA
[39] Jack P Gibbs, 'Crime, Punishment and Deterrence' [1968] *The South Western Social Science Quarterly* 48 (4) 515
[40] Joel Meyer, 'Reflections on Some Theories of Punishment' [1969] *Journal of Criminal Law and Criminology* (59) (4) 596
[41] S5 of the CPPA
[42] S 4 – 36 of CPPA
[43] S4 – 36 of CPPA

Billion, Eight Hundred million Naira.[44] The CPPA in having a low threshold for fines does little in crime deterrence. With its lenient sentencing model and low penalties fine, justice is perceived to go south and with the mouth watering amount that hackers make online. It's no rocket science that this crime is on the increase in Nigeria. Contrast the American case of *United States v Seleznev*[45] Seleznev was charged with wire fraud, intentional damage to a protected computer and was sentenced to 27 years in prison upon conviction.

More so, nearly all the provisions for offences requires proof of a specific intent, namely the intent to commit an illegal transfer of funds or data, the intent to commit a forgery, the intent to hinder the function of computer and/or telecommunication system, etc. the requirement to prove these specific intents significantly narrows the scope of each offence and makes proving each offence more difficult. for instance if an individual access a bank's computer and manipulates the records to make it appear that one account has been debited with N10,000.00 while another has been credited with N10,000.00 it may be argued, rightly, that such should be criminal in and of itself, under section 16(1) of the CPPA 2015. However, the prosecutor would have the additional burden of proving that manipulation of data was done for the specific intent of illegally transferring funds, if the defendant could successfully claim that he was a hacker who just wanted to see if he could actually manipulate bank data, such intent would be a defence to the charge. Mere cyber trespass itself should be criminal. The proliferation and seriousness of cyber criminality should accord it the status of strict liability offence as it is one of the most dangerous crimes in the world.[46]

Punitive and Onerous

One of the qualities of good law is the fact that it is corrective, rehabilitative and accessible than punitive. The application of the CPPA is punitive rather corrective or rehabilitative. The political class deliberately manipulated the provisions of the law to police journalists and suppress freedom of expression and thoughts, while abandoning its primary objectives the provisions of the Act have been used for the personal agenda and vendetta of politicians against the masses. S 24 which criminalizes cyber stalking is the black sheep section in the piece of legislation. S 24 CPPA is the new oppressive mode of repressing freedom of expression online in Nigeria.it has been used to gag and detain journalist cum bloggers making them an endangered species in Nigeria. Personal vendetta and online gagging of free speech is the least reason for enacting the CPPPA and indeed any law. If this were so, the State may become autocratic in its functioning, using the punishment to torment people. Authorities in Government have attempted to silence opposition views in the online media through arbitrary interpretation and abuse of the S 24 of the Act which addresses offensive statements on the internet. Bloggers and individuals have been arrested in this regard. Journalism is not an opposition; journalism is the oxygen of democracy and for the positive change and development of any democratic society.[47] In *IGP v Tim Elombah* accused persons online bloggers were accused of writing a derogatory article against the then IGP of Nigerian police termed 'IGP Ibrahim Idris's Unending Baggage of Controversies' ' they were arrested and charged to court. In 2022, 52 journalists were detained across the country under the CPPA.[48] The purpose of the CPPA was not to regulate the activities of journalists. Only free press can hold government accountable to the people. The Nigerian government should apply the law properly to cure the mischief for which it was enacted. In *SERAP v FRN*, the ECOWAS court ordered the Nigerian government to repeal S 24 of the CPPA by deleting provisions inconsistent with Nigeria obligation under the African charter on human and peoples right.[49] It has shown to be punitive rather than corrective.[50] In *Okedara v Attorney General of the Federation*[51] plaintiff lost his prayer to the court to declare s. 24 of the CPPA unconstitutional for violating the right to freedom of expression.

[44] Eyitayo Johnson, SFU Arrest Bank Hacker Over N1.87 Billion Fraud <https://www.specialfraudunit.org.ng/en/?p=1186> accessed February 5 2023

[45] Unreported, Russian cybercriminal sentenced to 27 years in prison for hacking and credit card fraud scheme, United States Department For Justice April 27 2019 < https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme> accessed February 5 2023

[46] Daniel Howley, Warren Buffet: Cyber Poses Real Threat To Humanity, April 30 2019 <https://finance.yahoo.com/news/warren-buffett-cyber-attacks> accessed 6th April 2023

[47] ibid

[48] Lawyer Calls For Amendment To Nigerian Cybercrime Act 'Manipulated To Suppress Free Press, Freedom of Expression'< https://saharareporters.com/2022/12/04/lawyer-calls-amendment-nigerian-cybercrime-act-manipulated-suppress-free-press-freedom> accessed February 5 2023

[49]ECW/CCJ/APP/09/19

[50]Emma Okonji, New Report Seeks Repeal, Re-enactment of Cybercrime Act 2015 <https://www.thisdaylive.com/index.php/2020/09/17/new-report-seeks-repeal-re-enactment-of-cybercrime-act-2015/> accessed February 5 2023

[51] Unreported Suit No. FHC/L/CS/937/17. According to Mr. Okedara in his pleadings stated. The last two years have been marked with cases of arrests, detentions and prosecutions of Nigerians in connection with speeches and expressions made on social media platforms ranging from Facebook posts to Tweets and to blogs. Some of the persons arrested, detained or being prosecuted have only acted within the purview of exercise of their Freedom of Expression as guaranteed in the 1999 Constitution (as amended).'

The CPPA places onerous regulatory and financial burden on the institutions it intends to protect. Particularly affected are financial institutions and service providers.[52] The principal responsibilities placed on financial institutions are contained in Part IV of the Act. The part places a duty to verify the identity of customers carrying out electronic financial transactions, requiring the customers to present documents bearing their names, addresses and other relevant information before issuing ATMs, credit or debit cards and other related electronic devices. Failure to do so attracts a fine upon conviction.[53] The duties placed on financial institutions to verify their customers' identities are onerous on these financial institutions. This duty represents a regulation of the financial sector that interferes with other regulators, particularly the CBN. It is particularly superfluous in light of the Bank Verification Numbers (BVN) policy which specifically provides for the biometric identification of bank users, making it a prerequisite for operating bank accounts in Nigeria.

Section 38 requires service providers to keep all traffic data and subscription for a period of at least two years. Further, service providers are required to turn over such information to law enforcement agencies and failure to comply with either attracts a fine of 7m naira. The responsibility of service providers to track and keep data on users is a regulatory load, particularly on the telecommunication sector, and interferes with the regulatory competence of the Nigerian Communications Commission (NCC). The measure is a duplication of efforts such as the SIM registration initiative and may indeed be redundant as the NCC is empowered by s.64 of the Nigerian Communications Act, 2003 to gather the same information. Section 21 creates a responsibility to report to the National Computer Emergency Response Team (CERT), any attacks, intrusions or other disruptions liable to hinder the functioning of another system or network. The section further empowers CERT to propose isolation of affected systems and networks. Additionally, failure to report any such incident within seven days is an offence rendering the offender liable to be denied internet services and a mandatory fine. The duty imposed by s.21 is potentially arduous, requiring the report of all attacks or disruptions to CERT. Yet the act itself provides no definition of these terms and makes no reference to the severity or success of the attack. [54]A financial institution, in its ordinary business may be subject to multiple attempted breaches or other disruptions. The requirement to report all such occurrences within seven days imposes a substantial duty on institutions and a mandatory fine is imposed for failure to do so. Additionally, CERT may further disrupt the institutions operations by denying it internet access under section 21(3).

The National Cyber-Security Fund is created by s.44 of the act. It is an account to be maintained with the Central Bank of Nigeria (CBN) and administered by the NSA. It is to be funded, *inter alia*, by a 0.005 levy on all transactions by businesses specified in the second schedule to the Act which are as follows: (i) GSM service providers and all telecommunication companies; (ii) internet service providers; (iii) banks and other financial institutions; (iv) insurance companies; and (v) the Nigerian stock exchange. This 0.5 per cent mandatory contribution to the fund on transactions carried out by certain service providers and financial institutions adds an extra cost to these businesses that will ultimately be passed to consumers. [55]The fund is at the discretion of the NSA and no indication on how it is to be applied is given in s.44 beyond stating in section 44(5) that up to 40 per cent of the fund may be allocated for programmes countering violent extremism.

Section 7 of the CPPA provides for registration of cybercafés by the CPPA. This defeats the entrepreneurial spirit of young and upcoming entrepreneurs who wish to invest in the cyber cafe sector. It is arduous for stakeholders in the cybercafé enterprise to pass through double registration. Having gone through the rigors of registering a business with the Corporate Affairs Commission to operate a cybercafé, it is daunting for cybercafe investors to be faced with another regulatory challenge of having to register with Computer Professionals' Registration Council. What this does to Small and Medium-scale Enterprises and the informal sector in Nigeria is that it kills entrepreneurial spirit. Nigeria should provide more concession to start up business to tackle the challenge of unemployment among youth. There should be no legal obstacle on the path for entrepreneurs. Of particular concern is the provision of section 19(3) which states 'Financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity'. This section is harsh and onerous on customers of financial institutions. To the extent that where there is a case of fraud against a financial institution, this section provides an escape route for such financial institution as proof of negligence is placed squarely on the shoulder of the customer. The shifting of this burden of proof is unjust. It is submitted that since the financial institution is in custody of the investments of the customer, and the customer is not privy to the security arrangements of the financial institution; the principle of *res ipsa loquitor* should apply in this respect.

[52] J Okoh, E Chukwueke, 'The Nigerian Cybercrime Act 2015 and its Implications for Financial Institutions and Service Providers' July 2016 <https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its implications-for-financial-institutions-and-service-providers#.ZGf2fHbMLIU> accessed February 5 2023
[53] Section 37(1)
[54] ibid
[55] ibid

Vagueness and Inelegant Draftsmanship

Vagueness of the CPPA in tackling cybercrime manifests in multifaceted angles, firstly in its title Cybercrimes (Prohibition, Prevention, ***Etc)*** [56]Act, 2015. The etc in the title makes it vague and open to series of interpretation and litigation. It also depicts legislative sloppiness. The title of an act should be concise brief and clear to exude the professionalism and care taken to enact the legislation. This is lacking in the CPPA. The opinion of whether a piece of legislation was professionally drafted is formed perusing the title of an Act. CPPA failed this all important test. Secondly another illustration of the vagueness of the Act is on the powers of investigation of law enforcement agencies (LEAS). The Act makes it difficult to choose which agency has the jurisdiction to investigate and prosecute cybercrime. The CPPA is silent on the specific law enforcement agency charged with prosecution of cybercrime.[57] There are multiple legislations in Nigeria at the moment covering financial crime, each empowering different agencies with powers to investigate and prosecute offenders. This often culminates into bottlenecks and clash of investigative and prosecutorial interests amongst the agencies.[58] The powers of Nigerian Police clearly set out in the Police Act empowers them to investigate and prosecute all offences in Nigeria,[59] while the Economic and Financial Crime Commissions Act sets up the Economic and Financial Crime Commission to investigate and prosecute all financial related crime in any court in Nigeria.[60]Regarding the prosecution of cases, there are conflicts between the Police, the Economic and Financial Crime Commissions, the Directorate of Public Prosecutions, and the Attorney-General.[61] All these bodies claim to derive their authorities to prosecute offenders for cybercrime in Nigeria from their enabling Acts.[62] In addition, Section 6 states that any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes *and* (emphasized) obtain data that are vital to national security, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than N5, 000,000.00 or to both fine and imprisonment. The wordings of the S 6 spews confusion as it is difficult to discern whether unlawful access mentioned in this section is in regarding to national security or unlawful access pertaining to data of citizens and companies.

Equally The Act in providing for punishments for offences in section 5(1) for example provides thus 'Any person who with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, shall be liable on conviction to imprisonment for a term of not more than 10 years without an option of fine.'[63]The phrase 'a term of not more than' used in this section as in many more sections of the Act means that the 'term' can be less. It could be interpreted to be a day, an hour, ten years or ten days. The judge is given a carte blanche which may lead to absurd sentences. That leaves the final sentence to the discretion of the Court. A mischievous judge could take the advantage of this loophole and mischievously hand down a one day sentence to a culprit and such pronouncement will still be within the ambient of the provision in this section. Term certain penalties will cure the vagueness malaise in the CPPA. An example of the provisions of Section 7(2)3) of the CPPA which prescribes punishment of N2, 000,000.00 or a 3 years jail is commendable. This approach should extend to all punishment sections of CPPA for clarity.

From all the foregoing, it is apparent that the state of this piece of legislation is not fit for purpose as a deterrent to cybercriminals. Another failing of the Act was in definitions.[64]

6. Conclusion

The CPPA has an objective of minimizing criminal activities in Nigeria. There has been repeated calls to have it repealed or in the very least amended. It is not normally good practice to call for repeal of laws except really obsolete and archaic laws that are no longer fit for purpose. The reason being that a lot of finances have been expended in enacting the law, a lot of effort was expended also. However the Fundamental Human Rights FHR of citizens is so sacrosanct that where a piece of legislation breaches it, there should be no compromise. The section/s/ of the CPPA that breaches FHR should be immediately repealed while The FHR compatible sections should be given the chance to test their efficacy in cybercrime prevention .Equally the onerous and punitive sections should also be repealed to bring about a fit for purpose legislation that is capable of regulating the Nigerian Cyber-ecosystem.

---

[56] Empahis added

[57] Obinne C. Obiefuna, Collins C. Ajibo & Emeka Adibe, 'Paradigm Shift In Cybersecurity Regulation In Nigeria: Barriers and Prospects', [2020],3 *Journal of Law Review*, 172

[58] Philip Ogu Ujomu, 'National Security, Social Order and the Quest for Human Dignity in Nigeria: Some Ethical Considerations' [2001] *Nordic Journal of African Studies*, 2, 245-264

[59] Etannibi E O Alemika, 'Police And Policing In Nigeria: Mandate, Crisis And Challenges' (2003) *The Nigeria Police And The Crisis Of Law And Order:* A Book Of Readings, 19-32

[60] Mohamed Chawki, 'Nigeria Tackles Advance Free Fraud' [2009] *Journal of Information Law & Technology*,9.

[61]Osita Mba, 'Judicial Review of the Prosecutorial Powers of the Attorney-General in England and Wales and Nigeria: An Imperative of the Rule of Law' [2010] *Oxford University Comparative Law* 7

[62] Obinne C. Obiefuna, Collins Ajibo & Emeka Adibe, Paradigm Shift In Cybersecurity Regulation in Nigeria: Barriers and Prospects, *Journal of Law Review* 2020(3) 184

[63] The vague sentencing language is not applicable only to S 5 CPPA but it cuts across most punishment sections

[64] Zakariya Adaramorala,Nigeria cybercrime and its loopholes, September 14 2015 <https://www.dailytrust.com.ng/nigerias-cybercrime-law-and-its-loopholes.html> accessed 6th May 2023