

# Cybercrime Prosecutors And Non-Retroactivity Of The Nigerian Cybercrimes Act 2015: Implication For The Administration Of Cybercrime Justice<sup>1</sup>

*Felix E. Eboibi*<sup>2</sup>

## **ABSTRACT**

The role of cybercrime prosecutors in the quest to eradicate the proliferation of cybercrime and enhance the administration of cybercrime justice in Nigeria cannot be overemphasized. However, the recent enactment of the Nigerian Cybercrimes Act 2015 which ordinarily should be a tool in the hands of cybercrime prosecutors, raises pungent questions as to the legality or otherwise of bringing pending cybercrime matters before courts and the prosecution of perpetrators of cybercrime prior to the commencement of the Act under the Nigerian Cybercrimes Act 2015. The dilemma that this portends for the administration of cybercrime justice is that in the absence of proper appreciation of the legal implications, a cybercrime prosecutor would amend ongoing cybercrime charges and arraign perpetrators of cybercrime for offences committed before the commencement of the Nigerian Cybercrimes Act 2015. This paper consequently analyses, from the perspective of legal inclinations, the appropriate role of a cybercrime prosecutor in respect to ongoing cybercrime proceedings prior to the commencement of the Nigerian Cybercrimes Act 2015. It

---

<sup>1</sup> Data de Recebimento:03/04/2018. Data de aceite: 18/06/2018.

<sup>2</sup> Felix E. Eboibi, Ph.D(Law), LL.M(Nig.), LL.B(Cal.), B.L(Nigerian Law School), Senior Lecturer, Faculty of Law, Niger Delta University, Wilberforce Island, Nigeria; Consultant on cybercrime prosecutions. E-mails: felixeboibi@mail.ndu.edu.ng or lixboibi@yahoo.com; Tel:+2348033175431.

unravels the apposite action for a cybercrime prosecutor when faced with an opportunity to arraign perpetrators of cybercrime prior to the commencement of the Act before the courts to enhance the effective administration of cybercrime justice.

**Key words:** *Cybercrime Prosecutors, Non-retroactivity, Nigerian Cybercrimes Act 2015, Administration of Cybercrime Justice, Cybercrime perpetrators.*

## 1. INTRODUCTION

Cybercrime entails a crime perpetrated in which a computer is used either as a tool or target or it involves elements of information technology infrastructure.<sup>3</sup> For an effective administration of cybercrime justice, the Nigerian cybercrime prosecutors being public authorities, whose acts are carried out in order to safeguard the society and in the interest of the public must endeavor to apply cybercrime law and its attendant penalties where it is observed in breach while putting into consideration the enshrined rights of cybercrime perpetrators.<sup>4</sup> Undoubtedly, the determination of the initiation or continuation of cybercrime prosecutions, conducting cybercrime prosecutions before courts and appealing or conducting appeals in respect to court judgments are within the purview of cybercrime prosecutors. In specific circumstances, cybercrime prosecutors engage in the conduct and supervision of investigations, gives assistance to victims, proffer alternative measures to cybercrime prosecution, and to national cybercrime policy implementation with the attendant adaptations to regional and local situations when the need arises and supervision of the execution of court judgments.<sup>5</sup>

---

3 F. E. Eboibi, *Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence* (2011) 10 *Nigerian Law and Practice Journal*, 139 at 140 - 141.

4 Council of Europe, *The Role of Public Prosecution in the Criminal Justice System, Recommendation Rec (2000)19* Adopted by the Committee of Ministers of the Council of Europe on 6 October 2000 and Explanatory Memorandum, 4, 14-15, Available at < <https://rm.coe.int/16804be55a>> Last accessed 23 March 2018.

5 *Ibid.*

Considering the aforementioned germane roles of cybercrime prosecutors in the administration of cybercrime justice, it is discernable that the onus and discretion to charge a cybercrime perpetrator for any cybercrime offence lies on a cybercrime prosecutor. Constitutionally, it is the Attorney-General and Minister of Justice of Nigeria, including law officers, under his supervision and special prosecutors permitted under enabling statutes or laws.<sup>6</sup> Based on the limitations placed on the review of this discretion, i. e, on bad faith or constitutional grounds, the cybercrime prosecutor's determination of preferring charges against cybercrime perpetrators impinges on their lives and liberty. Consequently, utmost care and diligence must be the watch word. Seeking and achieving justice and not deliberate attempt to convict at all cost should be the cybercrime prosecutors' role.<sup>7</sup>

The Nigerian Cybercrimes Act 2015 which commencement date is 15 May 2015 is a comprehensive cybercrime law put in place by the Nigerian government to regulate the conduct of users of cyberspace and perpetrators of cybercrime. The Act covers a broad spectrum of cybercrime offences punishable with penalties and fines in Part III, which includes; - Offences against critical national information infrastructure;<sup>8</sup> Unlawful access to a computer;<sup>9</sup> System Interference;<sup>10</sup> Interception of Electronic messages, e-mails, electronic money transfer;<sup>11</sup> Tampering with critical infrastructure;<sup>12</sup> Willful misdirection of electronic messages;<sup>13</sup> Unlawful interceptions;<sup>14</sup> Computer related

---

6 Constitution of the Federal Republic of Nigeria, 1999(As Amended), s.174; Cybercrimes (Prohibition, Prevention etc) Act 2015, s.41(2)(c) & 47; Economic and Financial Crimes Commission 2004, s.7.

7 Steven Chong, The Role And Duties Of A Prosecutor – The Lawyer Who Never “Loses” A Case, Whether Conviction Or Acquittal, being a paper delivered Legal Service Officers and Assistant Public Prosecutors, 2-5, Available at <[https://www.lawsociety.org.sg/.../Law%20Gazette/.../SLG\\_APR\\_20](https://www.lawsociety.org.sg/.../Law%20Gazette/.../SLG_APR_20)> Last accessed 24 March 2018.

8 Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s.5; see generally F.E Eboibi, A review of the legal and regulatory frameworks of the Nigerian Cybercrimes Act 2015 (2017) 33 Computer Law & Security Review, 700 - 717

9 *Ibid.*, s.6.

10 *Ibid.*, s.8.

11 *Ibid.*, s.9.

12 *Ibid.*, s.10.

13 *Ibid.*, s.11.

14 *Ibid.*, s.12.

forgery;<sup>15</sup> Computer related fraud;<sup>16</sup> Theft of electronic devices;<sup>17</sup> Unauthorised modification of computer systems, network data and system interference;<sup>18</sup> Cyber-terrorism;<sup>19</sup> Fraudulent issuance of e-instructions;<sup>20</sup> Identity theft and impersonation;<sup>21</sup> Child pornography and related offences;<sup>22</sup> Cyberstalking;<sup>23</sup> Cybersquatting;<sup>24</sup> Racists and xenophobic offences;<sup>25</sup> Importation and fabrication of e-tools;<sup>26</sup> Breach of confidence by service providers;<sup>27</sup> Manipulation of ATM/POS terminals;<sup>28</sup> Phishing, spamming, spreading of computer virus;<sup>29</sup> Dealing in card of another;<sup>30</sup> Purchase or sale of card of another;<sup>31</sup> Use of fraudulent device or attached e-mails and websites.<sup>32</sup>

However, prior to the enactment of the Act, cybercrime prosecutors in an attempt to curtail the menace of cybercrime proliferation in Nigeria, applied the Advance Fee Fraud and Other Fraud Related Offences (AFF) Act 2006 to prosecute perpetrators of cybercrime. It must be noted that the AFF Act was not repealed by the Nigerian Cybercrimes Act 2015. In this regard, there are pending cybercrime proceedings before the courts and also charges are yet to be preferred against other cybercrime perpetrators whose acts were committed prior to the commencement of the Nigerian Cybercrimes Act 2015. The question that arises is whether or not part heard charges on cybercrime offences under the AFF Act can be altered, amended and/or brought under the Nigerian Cybercrimes Act 2015 by cybercrime

---

15 *Ibid.*, s.13

16 *Ibid.*, s.14

17 *Ibid.*, s.15.

18 *Ibid.*, s.16

19 *Ibid.*, s.18.

20 *Ibid.*, s.20

21 *Ibid.*, s.22

22 *Ibid.*, s.23

23 *Ibid.*, s.24.

24 *Ibid.*, s.25.

25 *Ibid.*, s.26.

26 *Ibid.*, s.28.

27 *Ibid.*, s.29.

28 *Ibid.*, s.30.

29 *Ibid.*, s.32.

30 *Ibid.*, s.34.

31 *Ibid.*, s.35

32 *Ibid.*, s.36

prosecutors? On the other hand, can perpetrators of cybercrime offences committed before the commencement of the Nigerian Cybercrimes 2015 be charged under the Nigerian Cybercrimes Act 2015 by cybercrime prosecutors?

Basically, the answer to these questions is the crux of this research paper. This culminates in a determination whether in the cybercrime prosecutor's quest to administer cybercrime justice, is the cybercrime perpetrator not entitled to the right to be prevented from retroactive cybercrime laws. In which case, is the Nigerian Cybercrimes Act 2015 a retroactive cybercrime legislation? What then is the implication or otherwise of a retroactive cybercrime legislation and its effect on the administration of cybercrime justice?

A lack of appreciation of the foregoing, presents the likelihood of cybercrime perpetrators of denial of their constitutional right to prevention from retroactive laws and justice; possibility of being tried, convicted and sentenced under an unwritten and wrong cybercrime law; unwarranted amendment of part heard charges against cybercrime perpetrators by cybercrime prosecutors. This paper becomes very germane in order to avoid these.

Structurally, this paper, apart from introducing the role of a cybercrime prosecutor as it relates to the administration of cybercrime justice, it examines the development of cybercrime prosecution in Nigeria; the basis for prosecuting cybercrime perpetrators prior to the enactment of a comprehensive law on cybercrime. It thereafter examines the non-retroactivity of the Nigerian Cybercrimes Act 2015 and the role cybercrime prosecutors should play when faced with a new enactment. This paper ends with deductions and conclusion.

## **2 DEVELOPMENT OF CYBERCRIME PROSECUTION AND THE NIGERIAN CYBERCRIMES ACT 2015**

The absence of a comprehensive law on cybercrime is one reason that contributed to the proliferation of cybercrime in Nigeria. Howe-

ver, Nigeria prior to the enactment of the Nigerian Cybercrimes Act 2015, saw the popular fraudulent email scam attributed to the “yahoo boys” as a variant offence of obtaining property by false pretence proscribed under section 419 of the Criminal Code Act (now covered by the Advance Fee Fraud Act 2005 as amended in 2006, section 1 thereof). In this regard, cybercrime prosecutors could only prosecute perpetrators of advance fee fraud on the internet (online fraud) under the AFF Act 2006.

The establishment of the Economic and Financial Crimes Commission (EFCC) through the Economic and Financial Crimes Commission (Establishment) Act, 2004 attributed the power to investigate and prosecute all economic and financial crimes to EFCC. Section 1 of the AFF Act, 2006 is specifically against the perpetration of economic crime,<sup>33</sup> EFCC being the institution empowered to enforce the law.<sup>34</sup>

Based on the foregoing, prior to the enactment of the Nigerian Cybercrimes Act 2015, the EFCC (Establishment) Act 2004 specifically empowered the EFCC with particular reference to the AFF Act 2006 to investigate and prosecute perpetrators of cybercrimes in Nigeria. Thus, section 7(2) of the EFCC (Establishment) Act 2004, equipped the Commission with the responsibility of enforcing the provision of ‘... (b) *The Advance Fee Fraud and Other Fraud Related Offences Act 2006.*’<sup>35</sup> Typical instances of cybercrimes prosecuted in the form of online fraud in Nigeria by the EFCC are; Advance Fee Fraud Scam, Contract Scam, Inheritance or transfer Scam, Romance and Dating Scam, Employment Scam, Identity/Phishing Scam, Charity Scam, Lottery Scam, Crude oil/Mineral Resources sales Scam, Scholarship Scam, Car Auction Sale Scam, Immigrant/Visa Scam etc.

In *Mike Amadi v. Federal Republic of Nigeria*<sup>36</sup> where the Appellant (Mike Amadi) was charged before the High Court of Lagos

---

33 Economic and Financial Crimes (Establishment) Act, 2004, s. 1

34 *Ibid.* s. 7(2)

35 *Ibid.*

36 (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127

State holden at Ikeja by EFCC *inter alia* with attempt to obtain the sum of US\$125,000.00(One Hundred and Twenty Five Thousand United States Dollars from one Fabian Fajans by sending fake e-mails through his mail box princemike2001@yahoo.com, registered websites efcc-nigeria.com, Reddiff.com.India Limited, multilink telephone number 017946846 in respect to a forged Central Bank of Nigeria payment schedule containing false pretence by requesting for money to process the transfer of Two Million, Five Hundred Thousand United State Dollars (\$2.5 million USD) being the contract sum for the generators Fabio Fajans purported to have supplied the Federal Government of Nigeria for the All African Games 2003 and by falsely representing to Fabio Fajans that the said sum of US\$125,000.00 represent the five percent(5) processing fees of the total sum of USD 2.5 million contrary to sections 5(1), 8(b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act Cap. A6 Vol. 1, Laws of the Federation of Nigeria 2004 now 2006. On 20 May 2005 the High Court found him guilty and sentenced him to 16 years imprisonment. Aggrieved with the judgment of the High Court, the Appellant appealed to the Court of Appeal. The Court of Appeal affirmed the judgment of the High Court. On further appeal to the Supreme Court, the Supreme Court while dismissing the appellant's appeal, the judgment and sentences of the High Court and the Court of Appeal were affirmed.<sup>37</sup>

---

<sup>37</sup> See also Harrison Odiawa vs Federal Republic of Nigeria (2008) All FWLR (pt.439) 436; (2008) LPELR-CA/L/124/2006; Federal Republic of Nigeria (FRN) vs Benjamin Otoriomuo, Suit No. LCD/87C/2013, Judgement delivered on 8 October 2013 (Unreported); FRN v Ibiba Jack, Suit No. FHC/149C/2007, Judgement delivered on 13 February 2014 (Unreported).

Table one representation of cybercrime cases filed, convictions and pending cases between 2010 – 2014 based on available data (efcc)<sup>38</sup>

YEAR	NUMBER OF CASES FILED IN COURT	NUMBER OF CONVICTIONS RECORDED	<b>P E N D I N G CASES</b>
2010	151	17	134
2011	200	38	162
2012	187	49	138
2013	96	33	63
2014	106	59	47
<b>TOTAL</b>	<b>740</b>	<b>196</b>	<b>544</b>

The aforementioned cybercrime cases took place or are pending before the Nigerian Federal High Courts; States High Court and the High Court of the Federal Capital Territory (FCT) because according to the EFCC (establishment) Act and AFF Act 2006, the jurisdiction to the try cybercrime offenders is particularly granted to the Federal High Court or the High Court of a State or the High Court of the Federal Capital Territory (FCT).<sup>39</sup>

Pursuant to the enactment of the Nigerian Cybercrimes Act 2015, as stated earlier in this paper, comprehensive cybercrime offences punishable with penalties and fines are contained in Part III. Moreover, sections 41 (2), 47 and 50 of the Act empowers the Attorney General of the Federation and relevant law enforcement agencies to ensure effective prosecution of cybercrimes and cybersecurity matters under the Act, specifically before the Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed.

The problem that this development poses is that cybercrime prosecutors can decide to amend, alter and add to the charges of the

38 EFCC 2013 Annual Report, 21; Prince Madojemu Interview with Mr. C. A Ajah, staff EFCC policy, planning and strategy Department, Abuja, 25 April 2015.

39 EFCC (Establishment) Act, 2004, s. 19 (1); Advance Fee Fraud and Other Fraud Related Offences Act, 2006, s.14.

cybercrime cases pending before the various courts to reflect offences and penalties under the new Nigerian Cybercrimes Act 2015 definitely not covered by the AFF Act 2006. This is hinged on the ground that the alteration, amendment and addition in respect to any criminal charge in any criminal matter can be made at any time before judgment is given in the case.<sup>40</sup> Moreover, the cybercrime prosecutor may also decide to prefer charges against perpetrators of cybercrime for offences committed prior to the enactment of the Nigerian Cybercrimes Act 2015. Does these not contravene the constitutional right of non-retroactivity of crime or is the Nigerian Cybercrimes Act 2015 retroactive?

### **3 NON-RETROACTIVITY OF THE NIGERIAN CYBERCRIMES ACT 2015 AND THE ROLE OF CYBERCRIME PROSECUTORS**

In the exercise of the administration of cybercrime justice by cybercrime prosecutors, it is important for them to note that their role is subject to the constitutional right of a cybercrime perpetrator to be prevented from retroactive or retrospective cybercrime statutes or legislations. A cybercrime statute is deemed to be retroactive if it removes rights vested on a cybercrime perpetrator by a prior statute/law or makes a fresh responsibility, establishes a fresh obligation, or adds a fresh disability, bothering on already past events or activities.<sup>41</sup> Retroactive legislations also refers to *ex post facto* laws which by implication underscores laws that operates expressly or impliedly in order to impinge on acts perpetrated before they were enacted. In this regard, retroactivity simply makes an act a cybercrime which ordinarily was not a cybercrime as at the time it was committed.<sup>42</sup>

---

40 Young Ukauwa v. The State (2002) LPELR – 3325(SC).

41 Landgraf v. USI Film Products, 511 U.S. 244, 270 (1994); George Schoenwaelder, Retroactive Change in the Law to Punish a Defendant (November 2014) 30(4) Touro Law Review, 961–965.

42 Daniel Oran and Mark Tosti, Oran's Dictionary of the Law, (3rd Edition, West Legal Studies, New York, 2000), p. 178 cited in Bereket Alemayehu Hagos, (Non)retroactivity of Ethiopian Criminal Law, september 2015, 1, available at <[www.abysinnialaw.com](http://www.abysinnialaw.com)> Last accessed 23 March 2018.

The right to be protected from retroactive cybercrime statutes is discerned from two common law maxims: *Nullum crimen sine lege*: This maxim denotes that “no act is criminal except that defined to be so by the law” and *Nulla poene sine lege*: This maxim denotes that “no citizen can be made to suffer any punishment except in accordance with the law.”<sup>43</sup> The corollary is that cybercrime statutes should ordinarily be non-retroactive to ensure that cybercriminals or cybercrime perpetrators are not deprived of the fruits of natural justice. Hence, cybercrime prosecutors should apply the Nigerian Cybercrimes Act 2015 to acts of cybercrime committed after the Act came into force.

Generally, criminal statutes are enacted to operate prospectively on the premise that the legislature does not intend what is unjust.<sup>44</sup> This position is legalized under section 4(9) of the Constitution of the Federal Republic of Nigeria, 1999 (As Amended) – (The Nigerian Constitution) by stating unequivocally that the National Assembly or a House of Assembly shall not, in relation to any criminal offence whatsoever, have power to make any law which shall have retrospective effect. Section 36(8) of the Nigerian Constitution lays credence to the non-retroactivity of cybercrime legislations when it stated that no person shall be held guilty for any act or omission whatsoever that did not at the time the act or omission took place, constitute a crime, and no penalty should be given to an act unless the penalty that was in force at the time of the crime was committed. Moreover, section 36(12) of the Nigerian Constitution, expresses the fact that no person should be convicted for any crime except the crime is stated in a law and the punishment also provided. The crime in question should be known to law or expressly stated in an existing law.

Thus, in the case of *Omoju v. Federal Republic of Nigeria*,<sup>45</sup>the

---

43 Olanrewaju Olamide, The Basic Principles or Concepts of Criminal Law, available at <<https://www.djetlawyer.com/basic-principles-concepts-criminal-law/>> Last accessed 25 March 2018.

44 *Omatseye v. FRN* (2017) LPELR-42719(CA)

45 (2008) 7 NWLR pt. 1085, 38; see also, *George v. FRN* (2011) ALL FWLR pt 587, 664; *Amadi v. FRN* (2011) ALL FWLR pt. 561, 1588; *Aoko v. Fagbemi* (1961) 1 All NLR 400; In *Udokwu v Onugha* (1963) 7 ENLR 1, the act complained of was committed 6 months before they were prohibited by legislation.

appellant was arrested at the Nnamdi Azikiwe International Airport in Abuja by the NDLEA officials. Later, while in detention the appellant excreted 118 wraps of substances later confirmed to be heroine. The appellant was arraigned for the offence of exporting heroine and unlawful exportation of the said drug contrary to section 10 (b) of the Nigerian Drug Law Enforcement Agency Act. At the trial, the appellant pleaded guilty to the charges and was accordingly convicted and sentenced to two years imprisonment. Aggrieved by the judgment the appellant appealed to the Court of Appeal which dismissed the appeal. He later appealed to the Supreme Court wherein it was contended on behalf of the appellant that he was convicted under a non-existing Law in the section 10 (b) of the Nigerian Drug Law Enforcement Agency Act. In determining the appeal the Supreme Court considered the provision of section 36 (8) and (12) of the constitution and held; section 36 (8) and (12) of the 1999 constitution provides against retro-activity in legislation and punishing accused persons for offences not provided by the statute. In other words, under section 36 (8) and (12), a person cannot be punished for an offence which is not written.

However, a cybercrime prosecutor has the herculean task of determining whether a particular cybercrime legislation is a substantive law or procedural law. This is hinged on a fundamental principle of law that except it is expressly stated, no statute in respect to substantive law shall be construed so as to have retrospective or retroactive operation, unless it pertains to matters of procedure.<sup>46</sup> For instance, in *Elias v. Federal Republic of Nigeria & Anor.*,<sup>47</sup> the appellant was found guilty, convicted and sentenced contrary to Sections 1(2)(b) and 3(2) of the Miscellaneous Offences Act Cap M17 Laws of the Federation of Nigeria, 2004 and was ordered to refund the sum of N51.5 million

---

The court held that the accused had committed no offence by virtue of s.22(10), 1963 Constitution. 46 Afolabi V Gov. of Oyo State (1895) LPELR-196(SC) 1 at 54; Elias V Federal Republic of Nigeria & Anor, Suit No: CA/YL/141C/2015, Court of Appeal, Yola Judicial Division, Judgment delivered on Wednesday, the 29th day of June, 2016

47 Ibid

to the Adamawa State Local Governments Joint Account Committee Fund in accordance to Section 319 of the Administration of Criminal Justice Act (ACJA), 2015 by the Federal High Court, Yola. On appeal, the appellant contended that the provisions of the ACJA are not applicable as they cannot be applied retrospectively since the offence was committed in 2002. The Court of Appeal recognized that ACJA commencement date was 15 May 2015 and the offences for which the appellant was charged was committed in 2002 and 2003, and convicted in December 2015. The court held that “while substantive laws cannot be interpreted to have retrospective operation, when it comes to rules of procedure, it is permissible. Thus, the ACJA, being rules guiding the procedure of criminal trials in Federal High Courts and FCT High Courts, are capable of retrospective effect. The trial Court therefore acted rightly when it applied Section 319 of the ACJA to make an order on the Appellant to refund the sum of N51.5 million to the Adamawa State Local Governments Joint Account Committee.”<sup>48</sup>

Against the backdrop of the Nigerian Cybercrimes Act 2015, it must be noted that contrary to the *Elias* decision above, the Nigerian Cybercrimes Act 2015 is a substantive law which made provisions for cybercrime offences and penalties therein. Since the commencement date of the Nigerian Cybercrimes Act 2015 is 15 May 2015 and there are about 544 pending or part heard cybercrime matters before the courts prior to the commencement of the Act, cybercrime prosecutors cannot add, alter or amend the charges against the cybercrime perpetrators standing trial and introduce offences under the Nigerian Cybercrimes Act 2015. This would be contrary to sections 36(8) & (12) of the Nigerian Constitution and no cybercrime prosecutor should subject a cybercriminal through arduous and humiliating ordeal of cybercrime prosecution and to be so wrongfully convicted and punished for an on existing offence as at the time it was committed.<sup>49</sup>

---

48 Ibid

49 *Omatseye v. FRN (2017) LPELR-42719(CA)*

In the same vein, cybercrime prosecutors must resist the temptation of preferring charges against cybercriminals for cybercrime acts committed before 15 May 2015 pursuant to the Nigerian Cybercrimes Act 2015, especially where there is no express provision in the Act making it retroactive.

Cybercrime prosecutors must not allow the Nigerian Cybercrimes Act 2015 to affect pending cybercrime proceedings prior to the Nigerian Cybercrimes Act to deprive cybercriminals of their right to be prevented from retroactive cybercrime laws. The legal position is that it is the law in force or which is operational when the offence was committed that ought to be or is the applicable law.<sup>50</sup> In this regard, it is the Economic and Financial Crimes Commission (Establishment) Act, 2004 and Advance Fee Fraud and Other Fraud Related Offences Act, 2006. Any cybercrime trial and consequent conviction in breach of sections 36(8) & (12) of Nigerian Constitution and the principle of non-retroactivity of the Nigerian Cybercrimes Act 2015 is unconstitutional and any conviction thereon is liable to be set aside.<sup>51</sup>

The right to protection from retroactive cybercrime law underscores the fact or notion that individuals are entitled to such a right. It gives stability and certainty impetus to the justice system thereby facilitating the administration of cybercrime justice. The lack of accessibility and intelligibility of the Nigerian Cybercrimes Act 2015 is anchored on injustice against cybercrime perpetrators whose acts were not proscribed by the Act at the time they were committed. Obviously, at the time of commission of the cybercrime offence prior to the Nigerian Cybercrimes Act 2015, the Act was not accessible or knowable to cybercrime perpetrators. Most importantly, if cybercrime

---

50 Orgi v. FRN (2007) 13 NWLR (PT. 1050) 58 at 94; Kalango v Gov. Bayelsa State (2002) 17 NWLR (PT. 797) 617; Aremu v. Adekanye (2004) 13 NWLR (PT. 891) 972  
51 Aoko v. Fagbemi (1961) All NLR 400; Council Asake v. Nigerian Army Council (2007) 1 NWLR (Pt. 1015) 408; Udoku v. Onugha (1963) 2 All NLR 107; Prince Joshua Paulson V. The State (2011) LPELR - 4875 (CA); FRN & Anor. V. Lord Chief Udensi Ifegwu (2003) 15 NWLR (Pt. 542) 113; Major Adebayo V. Nigerian Army & Anor. (2012) LPELR - 7902 (CA); Hon. Hembe v. FRN (2014) LPELR - 22705 (CA)

prosecutors are allowed to alter, add or amend charges in respect to part heard cybercrime matters to reflect offences under the Nigerian Cybercrimes Act 2015 or charge cybercrime perpetrators for acts committed prior to the commencement of the Act, it will encourage abuse of individual rights.<sup>52</sup>

#### **4 CONCLUSION**

Cybercrime prosecutors cannot detach the rights of cybercrime perpetrators to be prevented from non-retroactive cybercrime laws in their quest to administer cybercrime justice. Considering, the recent enactment of the Nigerian cybercrimes Act 2015 and the 544 cybercrime cases pending in various courts, cybercrime prosecutors in charge of the cases are constitutionally prevented from altering, adding or amending on going charges in order to smuggle in cybercrime offences unavailable in the Advance Fee Fraud & Other Related Fraud Offences Act 2006, although prescribed under the Nigerian Cybercrimes Act 2015. In the same vein, it is unlawful for them to charge a cybercrime perpetrator under the Nigerian Cybercrimes Act 2015 for acts of cybercrime committed before 15 May 2015 when the Act commenced. Invariably, a cybercrime perpetrator can only be tried, convicted and sentenced for a cybercrime offence created and known to law at the time the act was committed.

#### **REFERENCES**

IKPANG, Aniedi J. Assessing the Principle of Legality in Nigerian Criminal Jurisprudence (2017) 58 **Journal of Law, Policy and Globalization**, 119 – 125.  
PISARI, Milana. Specialization of Criminal Justice Authorities in Dealing with

---

<sup>52</sup> James Popple, The right to protection for retroactive criminal law (August 1989) 13(4) Criminal Law Journal, 251 – 254; George Schoenwaelder, Above, note 39.

Cybercrime (2017) 2 *VARSTVOSLOVJE*, **Journal of Criminal Justice and Security**, 230-242.

OKENE, Ovunda V. C. Effective administration of Justice in Nigeria, Available at <[https://Works.Bepress.Com/Ovunda\\_V\\_C\\_Okene/36/](https://Works.Bepress.Com/Ovunda_V_C_Okene/36/)> Last Accessed 24 March 2018

WEAVER, Russell L. Retroactive Regulatory Interpretations: An Analysis of Judicial Responses (1986) 61(2) **Notre Dame Law Review**, 167-219.

SPIGA, Valentina. Non-retroactivity of Criminal Law (2011) 9 **Journal of International Criminal Justice**, 5 – 23.