

**THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT  
2015: LEGISLATIVE INEPTITUDE OR LACK OF TACT IN  
INTERNET MATTERS?**

**Aladokiye E. Gabriel- Whyte\***  
**Chukwuma O. Ajie\*\***

***Abstract***

*The internet is a means of communication by which users access information in cyberspace. The Cybercrimes (Prohibition, Prevention Etc) Act 2015 is the applicable statute by which offences are defined and punishment prescribed for offences committed in cyberspace or through the use or medium of the internet. Although the enactment of this statute a decade ago was largely welcome, a cursory look at its provisions and how littered offences are across the entire statute begs reason contrary to established legislative norms of carefully arranging similar provisions under specific subheads as is the norm. This paper analyzes each provision of the statute and co-ordinates kindred or related offences which ought to be under one sub-head and co-ordinates them accordingly without introducing new provisions. The paper concludes that although the enactment of the Cybercrimes (Prohibition, Prevention Etc) Act 2015 is a step in the right direction recognizing the pervasiveness of the internet in everyday Nigerian life, its current state begs reason and makes largely ineffective prosecution of offences contained therein.*

---

\* PhD (Nig.) LL.M (Nig.) B.L (Abuja); LL.B (Igbinedion); PGD, Education (IAUE); Notary Public and Senior Lecturer, Private and Property Law Department, Rivers State University, Nkpolu Oroworukwo, Port Harcourt.

\*\* PhD (RSU); LL.M (RSU) B.L; LL.B (RSU); Associate Professor, Commercial and Industrial Law Department, Rivers State University, Nkpolu-Oroworukwo, Port Harcourt; chukwuma.ajie1@ust.edu.ng

**Keywords:** Internet, Cyber, Cybercrime, Offences, Legislative

### **1.0 Introduction**

The nature of law being dynamic is such that it struggles to keep pace with scientific and technological development so as to continually regulate human conduct. This was the rationale behind the enactment of the Cybercrimes (Prohibition, Prevention Etc) Act 2015 which was welcome with the fact that Nigeria's legislature had recognized and welcome the use of internet in our *corpus juris* and recognizing the fact that offences could be committed utilizing the facility. However, the continued existence of the statute in its current state begs the question of legislative competence in its simplest sense not to talk about the question of properly appreciating the nature of the internet or cyber as properly called in the statute.

It is the norm in statute enactment that there are various sub-heads and delimitations for ease of understanding the statute not just to legal experts and professionals, but at least in the simplest sense to the citizenry whose conduct such statute intends to regulate. The current state of the statute with offences littered across various sub-heads is not only confusing for the legal mind, but questions the draftsman knowledge of the subject matter. Could this be as a result of lack of tact or knowledge on the subject matter or just merely legislative ineptitude giving room to several sections for punishment of offences to satisfy the political class? This paper proposes a more sensible arrangement of these sections already provided in the statute without making any new introductions or suggestions to make sense and restore the dignity of the legislature in carrying out its legislative functions on subject matters as sensitive and relevant as the cyber or internet is.

## 2.0 The Internet and Cyber Space

The internet has grown gigantic and amorphous and is incapable of a precise definition.<sup>1</sup> It is a network of networks created for the purpose of linking existing local networks to become accessible to every other global network host.<sup>2</sup> It is a global public space, an integral pillar of the modern economy<sup>3</sup> which is ‘borderless’ and omnipresent<sup>4</sup> since it is accessible to just anyone despite their location.<sup>5</sup> The internet is considered as the most global infrastructure in the history of humanity and unique in terms of accessibility, rich content and low cost in usage.<sup>6</sup> Some of its earliest visionaries conceived it as a platform for global discourse and a vector for a global civil society.<sup>7</sup>

The internet is a worldwide communication web created through technology, hardware and software and human use patterns which are

---

\* 08062949021

\*\* 08035536516.

<sup>1</sup> Thomas Haigh, Andrew L Russell and William H Dutton, ‘Histories of the Internet: Introducing a Special Issue of Information and Culture’ [2015] 50(2) *Information and Culture* 153-159, 144.

<sup>2</sup> Leslie Daigle, ‘On the Nature of the Internet’ [2016] *A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability* 15-32, 19.

<sup>3</sup> Annegret Bendiek, ‘Beyond US Hegemony: The Future of a Liberal Order of the Internet’ [2014] *German Marshall Fund of the United States* 57-69, 59.

<sup>4</sup> David D Clark, ‘The Contingent Internet’ [2016] 145(1) *The Journal of American Academy of Arts and Science* 9-17, 9.

<sup>5</sup> Andrea Slane, ‘Tales, Techs and Territories: Private International Law, Globalization and the Legal Construction of Borderlessness on the Internet’ [2008] 71(3) *Law and Contemporary Problems* 129-151, 129.

<sup>6</sup> Bendiek (n3) 64.

<sup>7</sup> Clark (n4) 14.

shaped by mores, customs and occasionally laws,<sup>8</sup> founded upon because of the divergent views on governance. It is operatively the most important public forum ever created,<sup>9</sup> its vast inter-connectivity far more nearly approximates the proto-typical “market place” of ideas.<sup>10</sup> The internet is defined as being borderless as a result of its technical feature which makes the same information accessible to users irrespective of location<sup>11</sup> thus making the world a global village indeed.<sup>12</sup> It is not a physical or tangible entity, rather it is a giant network that interconnects innumerable smaller groups of linked computer network and it is often referred to as a network of networks.<sup>13</sup>

Underscoring the importance and relevance of the internet, the Committee of Ministers of the Council of Europe sometime in 2007 in its recommendation of the public service value of the internet emphasized “access to and the capacity and ability to use the internet should be regarded as indispensable for the full exercise and enjoyment of human rights and

---

<sup>8</sup> Mary Mullen, ‘The Internet and Public Policy: Challenges and Policy Considerations for State Regulation’ [2018] *Information Brief, Research Department, Minnesota House of Representatives* 1-11, 2.

<sup>9</sup> *Denver Area Educ Telecomm Consortium Inc v FCC* 518 US 727, 802-3 (1996) (Kennedy J. dissenting).

<sup>10</sup> *Abrams v United States*, 250 US 616, 630 (1919) (Holmes J. dissenting).

<sup>11</sup> Andrea Slane, ‘Tales, Tech and Territories: Private International Law, Globalisation and the Legal Construction of Borderlessness on the Internet’ [2008] 71(3) *Law and Contemporary Problems* 129-151, 130.

<sup>12</sup> *Ibid* 131.

<sup>13</sup> Rikke Frank Jorgensen, ‘Internet Freedom and Expression’ [2000-2001] *European Master Degree in Human Rights and Democratisation Dissertation, Raoul Wallenberg Institute* 21.

fundamental freedoms in the information society.”<sup>14</sup> This stance may not be unconnected to the various uses of the internet.

The term Cyber or Cyber Space, though closely related to the term internet is technically different. Whilst the internet is a global network of interconnected computer networks; Cyber on the other hand refers to the virtual world created by this network encompassing all digital communication and computer systems. In other words, whilst the internet is physical infrastructure (cable, routers, modem etc.); cyber space on the other hand refers to the environment created by infrastructure where interactions and activities take place. However, for the purpose of this paper, either terms could be used interchangeably for ease of understanding and evading the complexities associated with the concept of internet and cyber uses.

### **3.0 Cybercrimes (Prohibition, Prevention, etc.) Act 2015**

The Cybercrimes Act is the first Nigerian legislation to deal with cyber security.<sup>15</sup> It is the argument of some scholars that the character of political leadership in Nigeria leads to the wrongful application of the Cybercrimes Act thereby undermining the independence of the Press.<sup>16</sup> The Act was introduced as a result of the associated difficulty with the prosecution of cyber related offences.<sup>17</sup> Cybercrimes as a term can be best understood as

---

<sup>14</sup> Council of Europe, ‘Committee of Ministers Recommendation on Measures to Promote the Public Service Value of the Internet’ (7 November, 2007), CM/Rec (2007), 16.

<sup>15</sup> Raymond Adibe, Cyril Chinedu Ike and Celestine Uchechukwu Udeogu, ‘Press Freedom and Nigeria’s Cybercrime Act of 2015: An Assessment’ [2017] 52(2) *Africa Spectrum* 117-127, 119.

<sup>16</sup> *Ibid* 117.

<sup>17</sup> *Ibid* 118.

crimes in which a computer is the object of the crime or is used as a tool to commit the offence.<sup>18</sup>

The Act in its Section 1 stated the Objective which is to provide an effective and unified legal, regulatory and institutional framework for the purpose of prohibiting, detecting, prosecution and punishment of cybercrimes; protecting critical national infrastructure and the protection of computer systems and network, electronic communication, intellectual property and privacy rights. The Act prohibits a number of cybercrimes with many of such offences being so closely related that understanding the differentiation between the offences may be difficult. To this end, the offences in the Act would be stratified to enable a bit of understanding even if it is admitted that the balkanization may be of little moment and is not by any means a water tight classification.

### **3.1 Cybercrimes by Persons Generally**

The Act prohibits and punishes the offence of meddling with critical national infrastructure to a term of imprisonment not exceeding 10 years without an option of fine and where in the process grievous bodily harm is occasioned, the imprisonment term becomes 15 years without an option of fine and where death occurs, it becomes life imprisonment.<sup>19</sup> In its Section 6, it prohibits unlawful access to a computer which contains vital information on national security for fraudulent purposes, whether the unlawful access is wholly or partly done is liable on conviction to an imprisonment term not exceeding 5 years or to a fine not exceeding ₦5,000,000.00 or both. It further provides that where the intent of having unlawful access to the computer is to obtain computer data or access any

---

<sup>18</sup> *Ibid* 119.

<sup>19</sup> Cybercrimes Act 2015, s 5.

commercial or industrial secrets or classified information such an offender would be liable to an imprisonment term of not more than 7 years or a fine not more than ₦7,000,000.00 or to both such fine and imprisonment term.<sup>20</sup>

Section 8 of the Act prohibits directly or indirectly hindering the proper functioning of a computer intentionally or for fraudulent purposes punishment for which would not exceed 2 years imprisonment or a fine not exceeding ₦5,000,000.00 or both. Similarly, a person who aborts or destroys any electronic mail is liable to 7 years imprisonment if such offender is a first time offender and to 14 years imprisonment on a second commission of the same offence.<sup>21</sup> Section 11 provides that any person who misdirects an electronic message with the intention of obtaining financial gain or cause delay or speed up the message with the intention of causing omission or commission that may defeat the purpose or essence of the message is liable to 3 years imprisonment or a fine of ₦1,000,000.00 or both. Where there is interception by technical means of computer data, electromagnetic emissions or computer signals, system or network carrying or emitting signals to or from a computer, the person causing the interception is liable to an imprisonment term not exceeding 2 years or a fine not exceeding ₦5,000,000.00 or both.<sup>22</sup>

Where a person or organization induces another person being in charge of electronic devices and in the employ of federal, state or local government to deliver to him emails, credit and debit card information commits an offence for which criminal liability is 2 years or a fine not more than ₦1,000,000.00 or both.<sup>23</sup> A person who accesses a computer and causes

---

<sup>20</sup> *Ibid* s 6 (1)-(4).

<sup>21</sup> Cybercrimes Act 2015, s 9.

<sup>22</sup> *Ibid* s 12(1).

<sup>23</sup> *Ibid* s 12(2).

inauthentic data to be read as authentic data commits an offence and is liable on conviction to an imprisonment term of 3 years imprisonment or a fine not less than ₦7,000,000.00 or both.<sup>24</sup> The same punishment is prescribed for person who without authority or in excess of same alters, suppresses or erases any data whether or not for economic benefit or himself or a third party.<sup>25</sup> For cases where the offender intentionally misrepresents facts to cause the recipient rely on such misrepresented facts and suffer damage or loss is liable on conviction to an imprisonment term not less than 5 years or to a fine not less than ₦10,000,000.00 or both.<sup>26</sup> Where a person forges or super scribes electronic messages or instructions, such a person is liable on conviction to a term of imprisonment not exceeding 3 years or a fine not exceeding ₦5,000,000.00 or both.<sup>27</sup>

Where a person modifies data in any computer system or network directly or indirectly, such a person shall be liable to an imprisonment term of not more than 3 years or a fine not more than ₦7,000,000.00 or both.<sup>28</sup> Where the act of the offender directly or indirectly hinders the functioning of a computer system by damaging, deleting, altering or suppressing the computer and making it not function as expected is liable on conviction to a term of imprisonment not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.<sup>29</sup> In cases where the offender utilizes electronic devices and forges another person's signature or company mandate, such would be liable to an imprisonment term of not more than 7 years or to a

---

<sup>24</sup> *Ibid* s 13.

<sup>25</sup> *Ibid* s 14(1).

<sup>26</sup> Cybercrimes Act 2015, s 14(2).

<sup>27</sup> *Ibid* s 14(3).

<sup>28</sup> *Ibid* s 16(1).

<sup>29</sup> *Ibid* s 16(3).

fine of not more than ₦10,000,000.00 or both.<sup>30</sup> Similarly, where a person produces, supplies or adapts any password, access code or any means by which security measure in a computer can be overcome is liable on conviction to an imprisonment term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.<sup>31</sup> Where the offence however is an intention or disclosure of a password to gain access, the offender becomes liable on conviction to an imprisonment term of not more than 2 years or a sum not more than ₦5,000,000.00 or both.<sup>32</sup> Where from the wrongful conduct loss or damage has occurred or the offender had utilized automated means to commit the crime, he becomes liable to an imprisonment term of not more than 5 years or a sum not more than ₦10,000,000.00 or both.<sup>33</sup>

Section 21 of the Act places a duty on persons and institutions operating a public or private computer system to immediately report attacks, intrusions or disruptions that hinder the functioning of any computer system or network to the National Computer Emergency Response Team (CERT) within 7 days of its occurrence, failure of which such person or institution would be liable to denial of internet together with paying a mandatory fine of ₦2,000,000.00 into the National Cyber Security Fund.<sup>34</sup> Where any person fraudulently or dishonestly makes use of another person's password, signature or other unique identification whether that other person is living or dead or impersonates that person to gain advantage or obtain interest in the property of that other person to his disadvantage; obstructs the course of justice or directly or indirectly makes false statement intending that it should be relied upon commits an offence and shall be liable on conviction

---

<sup>30</sup> *Ibid* s 17(1)(c).

<sup>31</sup> *Ibid* s 28(1).

<sup>32</sup> *Ibid* s 28 (2)(3).

<sup>33</sup> Cybercrimes Act 2015, s 28(4)(5).

<sup>34</sup> *Ibid* ss 21(1) and (3).

to an imprisonment term of not more than 5 years or a fine not more than ₦7,000,000.00 or to both such fine and imprisonment.<sup>35</sup>

Section 25 prohibits cybersquatting which entails intentionally taking or using a name, trademark, domain name or other word or phrase belonging to any individual or any other body corporate belonging to any of the tiers of government committed on the internet or any computer network without authority from the owners to so use and attracts an imprisonment term of 2 years or a fine not exceeding ₦5,000,000.00. It further prohibits any form of aiding, abetting, counseling or procuring anyone to commit an offence under the Cybercrimes Act with a penalty sum as provided for the principal offence.<sup>36</sup> The Act criminalizes sale or importation of any device that would lead to subversion of access codes or passwords with an imprisonment term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both whilst an intent or deliberately selling passwords or codes is punishable upon conviction to an imprisonment term of not more than 2 years or a fine not more than ₦5,000,000.00.<sup>37</sup> Other offences such as phishing, spamming, spread of virus or malware are also prohibited against under the Act and upon conviction, such offender is to be imprisoned for 3 years or a fine of ₦1,000,000.00 or both.<sup>38</sup>

### **3.2 Cybercrimes by Bank Officers and Private Sector Employees**

Where the person who tampered with critical infrastructure or electronic mail is an employee of a Local Government, private organization or financial institution such an offender will be held liable for an

---

<sup>35</sup> *Ibid* s 22(2)-(4).

<sup>36</sup> Cybercrimes Act 2015, s 27(1).

<sup>37</sup> *Ibid* s 28(1)-(3).

<sup>38</sup> *Ibid* s 32.

imprisonment term of 3 years or a fine of ₦5,000,000.00.<sup>39</sup> Where a person employed in private sector having a duty to pay out, manipulates a computer to short pay or over pay and actually so does to an employee of government or private sector, such a person is liable on conviction to a term not exceeding 7 years and shall forfeit proprietary interest in the sum stolen or property to the bank, financial institution or customer<sup>40</sup> or where the offender is employed in a bank or financial institution or acted in connivance with another person, in addition to the penalty prescribed, such a person is to refund the money stolen or forfeit property purchased with the stolen sum to the bank.<sup>41</sup> A person employed by a bank or other financial institution who with intent to defraud diverts emails shall be liable on conviction to a term of imprisonment not more than 5 years or fine not more than ₦7,000,000.00 or both.<sup>42</sup>

Any person or persons authorized to give access to employees to utilize computer and gives more than one access to a particular person or persons would be liable on conviction to 7 years imprisonment or ₦1,000,000.00 or both.<sup>43</sup> Where an officer of a financial institution charged with the responsibility of debit and credit or confirming electronic transfer, unlawfully and fraudulently issues false electronic or verbal messages is guilty of an offence and is liable to imprisonment for 7 years.<sup>44</sup> Thus in *UBA Plc v Vertex Agro Ltd*, the court held the bank liable for unauthorized debit from a customer's account and failure to reverse same 72 hours after

---

<sup>39</sup> *Ibid* s 10.

<sup>40</sup> *Ibid* s 14(4).

<sup>41</sup> *Ibid* s 14(4)(b); s 14(5).

<sup>42</sup> Cybercrimes Act 2015, s 14(4)(a).

<sup>43</sup> *Ibid* s 18(2).

<sup>44</sup> *Ibid* s 20.

compliant in consonance with Section 37(3) of the Cybercrimes Act 2015.<sup>45</sup> Where a person utilizes his special knowledge by virtue of working in a financial institution commits identity theft of its service provider, employer, staff or employee is liable upon conviction to 7 years imprisonment or ₦5,000,000.00 fine or both.<sup>46</sup>

Where an employee of a financial institution has manipulated an Automated Teller Machine (ATM) or Point of Sale (POS) machine for the purpose of defrauding another person, such an employee would be liable on conviction to 7 years imprisonment without an option of fine.<sup>47</sup> In situations where the bank official had counseled, procured, aided or abetted another person to commit an offence under the Cybercrimes Act, such an officer shall be liable to a term not more than 7 years and also be made to forfeit or refund to the person from whom the offence was committed such item that had been stolen or converted.<sup>48</sup> Where an officer in a financial institution is no longer in the services of his employer, he is expected to relinquish all access codes and passwords and where he fails to so do after disengagement is liable on conviction to 3 years imprisonment or a fine of ₦3,000,000.00 or both.<sup>49</sup>

### **3.3 Cybercrimes by Officers of Federal, State and Local Government**

Where the person who tampered with critical infrastructure or electronic mail is an employee of a Local Government, private organization or financial institution such an offender will be held liable for an

---

<sup>45</sup> (2020) 17 NWLR (pt 1754) 467.

<sup>46</sup> *Ibid* s 22(1).

<sup>47</sup> *Ibid* s 30(2).

<sup>48</sup> Cybercrimes Act 2015, s 27(2).

<sup>49</sup> *Ibid* s 31(2).

imprisonment term of 3 years or a fine of ₦5,000,000.00.<sup>50</sup> Where a person employed in the federal, state or local government or intentionally detains and hides electronic mails, credit and debit cards, messages, electronic payment found by him or delivered to him in error which known to the recipient ought to be delivered to some other person is liable on conviction to an imprisonment term of 1 year or a fine of ₦250,000.00 or both.<sup>51</sup> Where a person employed in public sector having a duty to pay out, manipulates a computer to short pay or over pay and actually so does to an employee of government or private sector, such a person is liable on conviction to a term not exceeding 7 years and shall forfeit proprietary interest in the sum stolen or property to the bank, financial institution or customer.<sup>52</sup>

#### **3.4 Cybercrimes Utilizing Automated Teller Machines (ATM), Point of Sale Machines (POS) and Bank Cards**

Any person who steals a financial institutions or public infrastructure terminal is liable on conviction to 3 years imprisonment or a fine of ₦1,000,000.00 or both.<sup>53</sup> Where the item stolen is an Automated Teller Machine (ATM), the imprisonment term is not more than 7 years or a fine not more than ₦10,000,000.00 or both,<sup>54</sup> whilst an attempt to steal an ATM is for a term not more than 1 year or a fine not more than ₦1,000,000.00 or both.<sup>55</sup> Where an ATM or Point of Sale (POS) machine is manipulated to defraud another, the offender would be held liable to 5 years imprisonment or a fine of ₦5,000,000.00 or both.<sup>56</sup>

---

<sup>50</sup> *Ibid* s 10.

<sup>51</sup> *Ibid* s 12(3).

<sup>52</sup> *Ibid* s 14(4).

<sup>53</sup> Cybercrimes Act 2015, s 15(a).

<sup>54</sup> *Ibid* s 15(b).

<sup>55</sup> *Ibid* s 15(c).

<sup>56</sup> *Ibid* s 30(1).

The Act in Section 33 criminalizes any use of credit card, debit card, loyalty card and other financial cards to obtain money, goods or services for the purpose of defrauding the card owner. The punishment prescribed for this crime is an imprisonment term of not more than 7 years or a fine not exceeding ₦5,000,000.00 or both together with liability to return or refund monetary value of whatever loss the card owner would have suffered. The use of counterfeit card; stolen card;<sup>57</sup> the sale of and purchase of cards other than by the issuer;<sup>58</sup> as well as fraudulently obtaining card information are all criminalized under the Cybercrimes Act.

### **3.5 Other Trans-Border Cybercrimes**

The Act established the offence of cyber terrorism by providing that any person that causes any computer, computer system or network for the purpose of terrorism would be liable on conviction to life imprisonment.<sup>59</sup> One major addition of the Cybercrimes Act is the inclusion of Child Pornography as an offence. The offence spans across producing, distributing or transmitting, procuring or possessing child pornography in a computer or computer data storage medium for which liability is 10 years imprisonment and a fine not exceeding ₦20,000,000.00 or both where the offence is for producing, offering or making available child pornography or distributing same. Whilst in situations of procuring for oneself or possessing it in a computer or computer data storage device, it is an imprisonment term not exceeding 5 years imprisonment or ₦10,000,000.00 or both.<sup>60</sup>

---

<sup>57</sup> *Ibid* s 34.

<sup>58</sup> *Ibid* s 35.

<sup>59</sup> Cybercrimes Act 2015, s 18(1).

<sup>60</sup> *Ibid* s 23(1).

Where there is unsolicited distribution of pornographic content, the person who so distributes shall be liable on conviction to 1 year imprisonment or a fine of ₦250,000.00 or both.<sup>61</sup> In situations where a person intentionally proposes, grooms or solicits to meet a child for the purpose of engaging in sexual activity with the child, such a person shall be liable on conviction to an imprisonment term of not more than 10 years and a fine of not more than ₦15,000,000.00.<sup>62</sup> Where the purpose of proposing, grooming or soliciting to meet the child is to engage in sexual activity with the child by using threats, force, inducement, abusing a position of trust, authority or influence over the child or the vulnerable situation of the child either on mental or physical disability suffered by the child; or to expose the child to participate in pornographic performance for profit or otherwise exploiting the child, such a person involved will be liable on conviction to an imprisonment term of not more than 15 years and a fine of not more than ₦25,000,000.00.<sup>63</sup>

The Act further prohibited the offence of cyber stalking which can be understood to mean where a person intentionally sends a message or other matter by means of a computer or network that is grossly offensive, pornographic, obscene or menacing character, false message for the purpose of causing annoyance, insult, injury, inconvenience, criminal intimidation, hatred, obstruction or needless anxiety would be held liable for an imprisonment term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.<sup>64</sup> It is further provided that bullying, threatening, harassing or threatening to kidnap or harm a person or

---

<sup>61</sup> *Ibid* s 23(2).

<sup>62</sup> *Ibid* s 23(3)(a) proviso (i).

<sup>63</sup> *Ibid* s 23(3)(b)(i)(ii),(c) proviso (ii).

<sup>64</sup> Cybercrimes Act 2015, s 24(1).

demanding a ransom by means of a computer makes the offender liable to an imprisonment term of 10 years imprisonment or a fine of ₦25,000,000.00,<sup>65</sup> on the other hand, where the threat is to harm property or reputation of any person, a deceased person, firm or organization the offence is punishable by an imprisonment term of 5 years or a minimum fine of ₦15,000,000.00.<sup>66</sup>

Distribution of racist and xenophobic materials, genocide or other crimes against humanity on the internet or other computer network are also prohibited under the Cybercrimes Act and punishable upon conviction to an imprisonment term of not more than 5 years or to a fine not exceeding ₦10,000,000.00.<sup>67</sup> Service providers are not excused from liability if they utilize their position to forge or defraud their consumers which makes such corporate organization being a service provider liable on conviction to a fine of ₦5,000,000.00 and forfeiture of the monetary value of the loss suffered by the consumer.<sup>68</sup> Where the service provider is a body corporate and the offence instigated by a director, secretary or other officer, the sentence shall be executed against that officer,<sup>69</sup> and where the service provider is an individual, he shall be liable on conviction to an imprisonment term of not more than 7 years and a fine of not more than ₦5,000,000.00 or both.<sup>70</sup>

---

<sup>65</sup> *Ibid* s 24(2) (a), (b)(i).

<sup>66</sup> *Ibid* s 24(2)(c)(ii).

<sup>67</sup> *Ibid* s 26.

<sup>68</sup> *Ibid* s 29(1).

<sup>69</sup> *Ibid* s 29(2)(a).

<sup>70</sup> Cybercrimes Act 2015, s 29(2)(c).

#### **4.0 Conclusion and Recommendations**

This statute has considered a welcome development to the legal regime on internet use in Nigeria howbeit with the challenges of not being properly co-ordinated identifying and tagging similar and kindred offences under one sub-head which is rightly identified in this paper. Although several charges have been preferred pursuant to the Cybercrimes Act including the very recent and popular case involving renown human rights lawyer and activist Dele Farotimi over internet defamation against Afe Babalola SAN,<sup>71</sup> the application of this statutes is beginning to be questioned which is arguably submitted stems first from the lack of legislative tact in properly identifying, tagging and labeling kindred offences. It is highly recommended that there should be a comprehensive overhaul and perhaps re-enactment of the statute with the five sub-heads as properly identified and christened thus-

- i. Cybercrimes by Persons generally;
- ii. Cybercrimes by Bank Officers and Private Sector Employees;
- iii. Cybercrimes by Officers of the Federal, State and Local Government Employees;
- iv. Cybercrimes Utilizing ATM Machines, POS Machines and Bank Cards; and
- v. Other Trans-Border Offences.

---

<sup>71</sup> Abiodun Sanusi, 'Police File fresh Charges against Dele Farotimi over alleged Defamation of Afe Babalola' *Premium Times* 6 December 2024  
<<https://www.premiumtimesng.com>> accessed 8 December, 2024.