

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)


---



---

**Computer Law  
&  
Security Review**


---



---

# A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015

Felix E. Eboibi \*

Faculty of Law, Niger Delta University, Wilberforce Island, Nigeria

## A B S T R A C T

### Keywords:

Nigerian Cybercrimes Act 2015  
Cybercrime offences and penalties  
Cybercrime institutions and  
governance  
Jurisdiction  
Mutual assistance

As a sequel to the liberalization of the Nigerian telecommunication sector in late 1990s, Nigeria experienced tremendous growth in telecommunications usage and internet penetration because of the proliferation of Internet Service Providers (ISPs) and Cybercafés. Consequently, fraudsters started using the internet, instead of the regular mails and fax 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. The Nigerian government became alarmed with the misuse of the cyberspace by the fraudsters and based on the quest to tackle the menace inaugurated in 2003 a Presidential Committee and subsequent initiatives to investigate the activities of these fraudsters on cyberspace and fashion out a legal and regulatory framework to circumvent the menace of cybercrime. Unfortunately, it took the Nigerian government over a decade to enact a cybercrime legal and regulatory framework after being exposed to the severe negative implications for national economic development, national security, international relations and also human rights and human security. This paper examines Nigeria's legal and regulatory response to cybercrime. It espouses an analysis of the adequacy of the legal and regulatory frameworks in existence to curtail cybercrime in Nigeria.

© 2017 Felix E. Eboibi. Published by Elsevier Ltd. All rights reserved.

## 1. Introduction

Cyber criminality only became an issue in the Nigerian legal system, only few years back. In the early 1980s, the perpetuation of advance fee fraud in Nigeria metamorphosed through the use of fax and handwritten letters and the postal office as

a delivery agent to victims of perpetrators.<sup>1</sup> Consequent upon the extension of internet services to Nigeria in the late 1980s and early 1990s, fraudsters migrated to the use of the internet, even though internet services were expensive and beyond the reach of most ordinary Nigerians.<sup>2</sup> At this time, Internet service was only available through the Nigerian Government owned Telecommunication Company and this restricted access

\* Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria.

E-mail addresses: [felixeboibi@mail.ndu.edu.ng](mailto:felixeboibi@mail.ndu.edu.ng), [lixboibi@yahoo.com](mailto:lixboibi@yahoo.com).

<sup>1</sup> F.E Eboibi, Enforcement of Cybercrime in Nigeria: Are We Still Having Teething Problems? Being a paper presented in a Certificate Training Course/Conference; *Cybersecurity, Sovereignty, and Democratic Governance in Africa* organized by the Council for the Development of Social Science in Africa, Democratic Governance Institute, Dakar, Senegal, 27 July–7 August 2015, 1–2.

<sup>2</sup> Ibid.

<http://dx.doi.org/10.1016/j.clsr.2017.03.020>

0267-3649/© 2017 Felix E. Eboibi. Published by Elsevier Ltd. All rights reserved.

to the use of internet services.<sup>3</sup> This prompted the deregulation of the telecommunications sector in the late 1990s and more private Internet Service Providers (ISPs) and Cybercafés were licensed. The licensing of private providers improved availability and access became less expensive. An increase of ISPs and Cybercafés was experienced in the country. Moreover, the Nigerian Government in 2001 commissioned a body of experts to design a National Policy on Information Technology (NPFIT).<sup>4</sup> All these brought about the robust availability of mobile phone services, a liberalized telecommunications sector and internet service business. Youths were trained in IT skills, quite a number of unemployed and underemployed citizens became gainfully employed and self-employed in the ICT sector; and cybercafés sprung up in every part of the country.<sup>5</sup>

Criminals utilizing the internet to perpetrate all manner of cybercrimes quickly followed this. Cybercrime is a type of online crime in which the computer is used as either a tool or target or involving information technology infrastructure.<sup>6</sup> The different categories of cybercrime commonly perpetrated were electronic auction or retail-based fraud schemes, stock scams, work at home scams and on-line (e-mail) advance fee fraud scams, web cloning, piracy, phishing, online lottery fraud, job scams, identity theft, credit card fraud, impersonation, fraudulent loan scams, romance scams and hacking.<sup>7</sup> The advance fee e-mail scheme is the most common form of internet fraud from the Nigerian perspective. The messages are often referred to as “Nigerian” or “419” cyber scams because the emails often come from individuals who purport to reside in a foreign country – Nigeria.<sup>8</sup> Human weakness and the greed to succeed together with the use of sophisticated technological applications grossly impacted on the success in the activities of these Nigerian cybercriminals.

The Nigerian Supreme Court has had course to entertain an online Advance Fee Fraud case; *Mike Amadi vs Federal Republic of Nigeria*<sup>9</sup> where the Appellant (Mike Amadi) was charged before the High Court of Lagos 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). This was from Fabian Fajans by sending fake e-mails through his mail box [princemike2001@yahoo.com](mailto:princemike2001@yahoo.com), registered websites [efccnigeria.com](http://efccnigeria.com), [Reddiff.com](http://Reddiff.com). India Limited, multilink telephone number 017946846 in respect of a forged Central Bank of Nigeria payment schedule containing false pretence. It was perpetrated by requesting money to process the transfer of \$2.5 million USD being the contract sum for the generators. Fabio Fajans was 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 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.

Thus, this period heralded Nigeria being nicknamed in domestic and international reports/literatures as the hub of cybercrime and cybercrime perpetrators:<sup>10</sup>

- In 2002 the Internet Fraud Complaint Centre published a report which established that Nigeria was ranked second in the world among top ten countries and first in Africa in cybercrime perpetration with a rating of 5.1%; United States of America (USA) is first with 76.7% rating, followed by Canada second with 3.5% rating.<sup>11</sup>

<sup>3</sup> M.U Maska, Building National Cybersecurity capacity in Nigeria: The Journey So Far. Being a paper presented at the Regional Cybersecurity forum for Africa and arab States, Tunis 2009, 4; Ahmed Sa’ad Abubakar, Investigating Fraud Schemes in Nigeria. Being a paper presented at the International Conference on Cooperation Against Cybercrime, Organized by the Council of Europe, Strasbourg, 10–11 March, 2009, 2.

<sup>4</sup> F.E. Eboibi, As above, note 1.

<sup>5</sup> Ibid.; See Roseline Obada Moses-Oke, ‘Cyber Capacity without Cyber Security: A Case Study of Nigeria’s National Policy for Information Technology (NPFIT),’ *Journal of Philosophy, Science & Law*, May 30 2012, vol. 12 ([www.miami.edu/ethics/jpsl](http://www.miami.edu/ethics/jpsl)) 20 April 2015.

<sup>6</sup> F.E. Eboibi, Legal Approach to Computers in Cybercrime Enforcement in a Changing World (2014) 13 *Nigerian Law and Practice Journal*, 36.

<sup>7</sup> Ibid.; See U.J. Orji, *Cybersecurity Law and Regulation* (The Netherlands: Wolf Legal Publishers, 2012), 488–489.

<sup>8</sup> F.E. Eboibi, As above, note 1. See also F.E. Eboibi, Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence (2011) 10 *Nigerian Law and Practice Journal*, 139–160.

<sup>9</sup> (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127. See also *Harrison Odiawa vs Federal Republic of Nigeria*(2003–2010) ECLR 19–99; (2008) All FWLR (pt.439) 436; (2008) LPELR-CA/L/124/2006.

<sup>10</sup> Ibid; See Wolf Pack & Digital Jewels, 2014: The Nigerian Cyber Threat Barometer Report, 4,6, Available at <<https://www.digitaljewels.net/index.php/resource-center/djlnews/129-the-2014-nigerian-cyber-threat-barometer>> (Accessed 4 April 2015); A Loucif Kharouni, Africa: A New Safe Harbor for Cybercriminals? Trend Micro Incorporated Research Paper, 2013, 1, Available at <<http://www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf>> (Accessed 10 April 2015); E.E Adomi & S.E. Adomi, Combating Cybercrime in Nigeria, (2008) vol. 26(5) *The Electronic Library*, 718; Internet Crime Complaint Center, 2010 Internet Crime Report (National White Collar Crime Complaint Center: United States, 2011), 11, Available at <<http://www.nw3c.org> or [www.ic3.gov](http://www.ic3.gov)> (Accessed 9 April 2015); Seun Ayantokun, Nigeria needs Anti-Cybercrime Law now – Minister (Tuesday 15 November 2011), Available at <<http://www.tribune.com.ng/index.php/tele-info/31205-nigeria-needs-anti-cyber-crime-law-now-minister>> (Accessed 3 April 2015); Agih L. & Mibzar B., Nigeria: Cybercrimes-Nation Ranks Third in the World (3 February 2010) Available at <<http://www.alafrika.com/nigeria>> (Accessed 2 April 2015); Eric Agwe-Mbarika Akuta, et al., Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy & Practice (May 2011) vol.1(4) *Journal of Research in Peace, Gender and Development*,129,132; Okonigene Robert Ehimen & Adekanle Bola, Cybercrime in Nigeria (2009) vol.3(1) *Business Intelligence Journal*, 95,97.

<sup>11</sup> National White Collar Crime Center and the Federal Bureau of Investigation, IFCC 2002 Internet Fraud Report January 1, 2002–December 31, 2002, (The National White Collar Crime Center, 2003), p.8, ([http://www.ic3.gov/media/annualreport/2002\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2002_IC3Report.pdf)) 10 July 2015.

Download English Version:

<https://daneshyari.com/en/article/4957850>

Download Persian Version:

<https://daneshyari.com/article/4957850>

[Daneshyari.com](https://daneshyari.com)