24

EBONYI STATE UNIVERSITY
LAW JOURNAL

Volume 6 No. 1, 2015 **ISSN: 0794-926X**

Legal Framework on the Determination of the Paternity of a Nigerian Child An Eagle That Cannot Fly?	*Dr. M. A. Ajanwachuku and C. C. Nwogbo-Egwu*	1
Understanding The Role of the United Nations Environment Programme in Global Environmental Protection	*Omaka Chukwu Amari, Ph.D and Uguru Uchechukwu*	10
Climate Change: A Review of the Legal Framework Against Practices That Enhance Global Warming In Nigeria	*Atsegbua, L., SAN, & Daudu, S. O.,*	22
The Challenges to Enforcement of Environmental Protection Regulations in Nigeria's Non-Oil Sector	*Dr. (Mrs.) Violet O. Aigbokhaevbo Mrs. Edoghogho Ewere*	37
Sustainable Development in United Kingdom And Canada: Critical Lessons For Nigerian Enviromental Policy Makers.	*Uchechukwu Uguru*	50
Environmental Pollution and Violation of the Right to Health: A Case Study of Niger Delta of Nigeria	*Abdulkadir Bolaji Abdulkadir (PhD)**	71
The Nigeria Police and the Menace of Armed Robbery: A Legal Panacea	*A.O. Filani*	83
Defects of the Compensation Provisions under the Land Use Act: The Need For Review.	*Ogah, C. C.*	91
The Dilemma of the Concept of "Fundamental Breach" under the UN Convention on International Sale of Goods (CISG).	Ituma, Chibueze Calistus	99

A Publication of the Faculty of Law, Ebonyi State University, Abakaliki, Nigeria

EBONYI STATE UNIVERSITY LAW JOURNAL

Volume 6 No. 1, 2015

ISSN: 0794-926X

The Separate Legal Personality of a Company: A Legal Paradox	Eseni A. Udu,	114
Demystifying the Provisions of the Land Use Act Of 1978	*Ituma, Chibueze Calistus*	127
Combating Crimes In Cyberspace: Examining The *(in)adequacy* of the Criminal Code Act And The Criminal Procedure Act	*IkengaK.E.Oraegbunam, PhD*	138
The Nigerian Response to the Casualties of its Petroleum Industry	*Dr. (Mrs.) Mobolaji P. Ezekiel & J.O. Garuba*	153
Impeachment under the Nigerian Constitution: An Appraisal	*Dr. J. A.M.Agbonika*	164
The Nigerian Personal Income Tax (Amendment) Act 2011: Issues and Controversies	*Gasiokwu Peter Ikechukwu Ph.D*	176
Rethinking Legislative Immunity In Nigeria	Gabriel O. Arishe	185
An Appraisal of the Doctrines of Exhaustion, Ripeness and Locus Standi as means to Preventing Frivolous Action Against Administrative Decisions In Nigeria	*Ilias B. Lawal & Sunday A. Fagbemi*	201
Evolving Measures Towards the Security of Employment In Nigeria: A Legal Perspective	*J. O. Odion*	217
Unemployment and Security Implications: Overcoming the Problem of Unemployment Through A Good Tax System In Nigeria	*Nnaemeka .B. Amadi*	228
Citizenship and Diaspora Voting Rights	Okpeahior A. Rita; Ph.D.,	236

IKENGA ORAEGBUNAM & CO.
SOLICITORS AND ADVOCATES
VERITAS ET VITA LAW OFFICE
NIGERIA
SIGNATURE
DATE

First Published 2005
VOLUME 6 NO. 1 2015 EBONYI STATE UNIVERSITY LAW JOURNAL

© Faculty of Law, Ebonyi State University, Abakaliki Nigeria

This Journal is published twice yearly

All rights reserved. No part of this publication may be reproduced, stored system, or transmitted in any form or by any means, electronic, mechanical, recording or otherwise without the prior permission of the Publisher.

ISSN 0794-926X

Printed by:
Ronic Publication
@ 08039560061, 08051332399
Contact 2 Isielu Street
Abakaliki
Ebonyi State

EBONYI STATE UNIVERSITY LAW JOURNAL

Dean of Law Dr. M. A. Ajanwachuku

Editor-in-Chief Prof. C. A. Omaka

Editorial Board
Prof. C. A Omaka
Prof. Andrew I. Chukwuemerie
U. Uguru
H. P. Faga

Advisory Editorial Board
Prof. R. A. C. E. Echara
Prof. Yemi Akinseye-George
Prof. I. F. Fekumo
Prof. Ernest Ojukwu
Prof. E. S. Nwauche
Prof. M. O. Udombana

IKENGA OKAEGBUNAM & CO.
SOLICITORS AND ADVOCATES
VERITAS ET VITA LAW OFFICE
AVENUE ST. AUGUSTINE CATH. CHURCH IMPOR
NIGERIA
SIGNATURE
DATE

COMBATING CRIMES IN CYBERSPACE: EXAMINING THE *(IN)ADEQUACY* OF THE CRIMINAL CODE ACT AND THE CRIMINAL PROCEDURE ACT

IkengaK.E.Oraegbunam, PhD[*]

Abstract

This study undertakes a review of the relevant provisions of the Criminal Code Act and the Criminal Procedure Act in view of ascertaining the adequacy, or otherwise, of the statutes in fighting crimes committed in cyberspace in the relevant territorial jurisdiction. This would only serve as a case study of the paucity of the necessary legal regime that is needed to combat cyber criminality in Nigeria today. Thus, cognizant of the enormous positive role of the internet and allied applications in enhancing the quality of human life today, this inquiry is not unaware of the reality of criminal behaviours via same. This paper culminates in practical suggestions that would peter out an adequate, comprehensive, and effective anti-cybercrime legal framework.

1. Preamble

The emergence of the internet and the development of computer technology have added a great deal to the quality of human life in the contemporary world. The internet today touches every aspect of human life irrespective of location in the globe. Thanks to the computer and the internet, the prophecy of McLuhan[1] as far back as the 1960s about the world becoming 'a global village' is all the more fulfilled today with precision. Hence, the contemporary world is knitted together not just as a 'global village' but more aptly as a 'global sitting room', so to speak. Daily activities of human beings are increasingly affected in form, size, content and time by the computer and the internet in quite positive way. The result is that the benefits of the attendant information revolution are very well extended to all. Banking, commerce, contract, communication, publication, education, research, marketing and so on, are enhanced and facilitated by computer technology and its products.

Moreover, as advancement in information and communication technology (ICT) has led to the representation of different types of information in electronic format, graphics, texts, pictures and voice can all be digitized.Akomolede notes that, for instance, "many difficulties

[*]Ikenga K. E. Oraegbunam, PhD (Laws), PhD (Rel. & Soc.), PhD (Phil.), MEd, BL, Senior Lecturer, Department of International Law & Jurisprudence, Faculty of Law, NnamdiAzikiwe University, Awka, Nigeria. E-mail: ikengaken@gmail.com.

[1]McLuhan, E. "The Source of the Term, "Global Village" Retrieved fromhttp://projects.chass.utoronto.ca/mcluhan-studies/v1_iss2/1_2art2.htm. Last visited on 25-10-14.

which hampered international and even national commercial transactions in the past have now been consigned to the dust-bin of history".[2] Along with these geometric changes in information presentation and distribution are tandem demands in user expectations for more rapid, open and global access to information than has been available in the past.In recent times, with the explosion of GSM telephony services in Nigeria, which saw many networks upgrading their services, social media like Facebook and Twitter became commonplace overnight. It is now common to hear refrains like "I'll link you up on Facebook", or "That tweet from you was natty", etc. Now that handheld devices, especially smart phones are almost everybody's *vade mecum*, it is now commonplace to see people, especially youths permanently glued to their devices, in buses, eateries, in aircraft – anyplace--chatting or browsing from one site to the other. With billions of people on Twitter, Facebook, LinkedIn and others, trillions of words and billions of images are flying through cyberspace every second as multitudes communicate, chatting, sending SMS and MMS.

However, the advent of the internet and the proliferation of digital regime have also created new opportunities for those who engage in illegal activities. Among these illegalities, criminality occupies the prime position. Magnin observes that "during the last twenty years, smart computer users using their machine to commit crimes have fascinated the world and generated a strange feeling composed of admiration and fear".[3] Hence, the sophistication in technology, cybernetics and computer communication has not only produced a dramatic increase in the incidence of criminal activities but has also resulted in the evolution of what seems to be new varieties in criminality. Certainly, old forms of crimes such as fraud, gambling, piracy, forgery, cheating, terrorism, criminal defamation, stealing, and the like, receive more boost and fillip as a result of the speed, convenience and worldwide coverage of the internet. More still, new types of offences like electronic mail scams, cyber stalking, page jacking, salami attacks, internet time theft, electronic mail bombing and spoofing, unauthorized access to computer systems or network, and so on, are created and aided by same qualities.

There is no gainsaying that in Nigeria today, the adoption of computer/internet system, and computer appreciationare on the increase. This follows the identification of information and communication technology as an essential tool for sustainable development. Consequently, internet usage in Nigeria has grown rapidly resulting in the explosion of Internet Service Providers (ISP) and Internet access points. This has had several positive impacts on the socio-economic and educational developments in the country. No wonder, recently, the federal government created the Ministry of ICT. Unfortunately, this shift from traditional communication medium to the new electronic system seems to also constitute a threat to national and institutional growth by providing a platform for internet criminal activities. For instance, Longe and Chiemeke observe that "the country's image has suffered as a result of the nefarious

[2]Akomolede, T. I., "Contemporary Legal Issues in Electronic Commerce in Nigeria", *Potchefstroom Electronic Law Journal*, 2008 (3).Retrieved from http://www.ajol.info/index.php/pelj/article/view/42234/9353. Last visited on 30 - 06 – 12.

[3]Magnin, C.J., *The 2001 Council of Europe Convention on Cyber – Crime: An Efficient Tool to Fight Crime in Cyber – Space*, LL.M Dissertation Santa Clara University, June 2002, p.1. Retrieved from http://www.magnin.org/publications/2001.06.scu.Last visited on 01-08-11.

activities of some Nigerians that have now turned the internet into a cheap channel for the perpetration of criminal spamming activities known as the Advance Fee Fraud".[4]

In fact, the phenomenon of cyber criminality is on the alarming stage in Nigeria today. Global statistics show that Nigeria ranks very high in this regard.[5] In Nigeria, it is commonplace to find a good number of youths often on daily basis, flocking cyber cafés for criminal enterprise, for which reason these young often unemployed persons have been referred to as "yahoo boys". The vicious activities of these miscreants have adversely affected all aspects of Nigeria's national and international life with the toll they take on individual development. In what immediately follows, this paper will do a critical review of the Criminal Code Act and the Criminal Procedure Act, governing as it were the criminal prosecution and adjudication in Southern Nigeria, with a view to demonstrating the extent of the role of criminal statutes in fighting cyber criminality in Nigeria today. Relevant practical suggestions will capitulate the jurisprudential discourse.

2. Criminal Code Act[6]

The Criminal Code Act is a product of the colonial government in Nigeria. The Act embodies a clearly worded, concise, and unified set of criminal law principles which need was felt by the British colonial administration to replace the relatively complicated and not easily ascertainable common law of crime governing the colony of Lagos, on the one hand, and the varieties of customary criminal laws in other parts of the larger colony[7], on the other hand. Hence, in 1904 the Lugard administration in the North introduced by proclamation a criminal code which purpose was to declare, consolidate and amend the criminal law. By June 1, 1916 a Criminal Code Act which long title read "An Act to establish a code of criminal law", was extended to the whole country sequel to the 1914 amalgamation of the Northern and Southern protectorates. The code received a major alteration in 1945.[8] The operation of the code was later geographically confined to the southern part of Nigeria as a result of pro-Islamic protests and sensibilities in the North which petered out in the enactment of the Penal Code in 1959 with its Sharia bias. However, what is known as the criminal code which provides for the crimes and their punishments is only a schedule to the seven-section Act.

Nevertheless, it is an incontestable fact that at the time of the enactment or adoption of major amendment of the Criminal Code, the development and use of the computer system was at best at its rudimentary stage. The internet was virtually non-existent. Therefore, the code could

[4]Longe, O.B. and Chiemeke, S.C., "Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points Playing?", *European Journal of Social Sciences*, vol. 6, No. 4, 2008, p. 132.

[5]*Ibid.* See also Malakata, M., *Nigeria Cybercrime Ranking Stirs Fears about Investments*. Retrieved from http://news.idg.no/cw/art.cfm? Id = BE74BCD7-1A64-67EA-E4IFF3. Last visited on 01-06-11. See also Osodo, I.,*Nigeria Ranked 70th in Cyber Crime*. Retrieved from http://www.itnewsafrica.com/2010/05/nigeria-ranks-70-in-cyber-crime/ Last visited on 01-06-11.

[6]*Criminal Code Act*, Cap. C. 38 Laws of the Federation of Nigeria 2004.

[7]Okonkwo, C. O., *Criminal Law in Nigeria*, 2nd Ed., Spectrum Books Ltd., Ibadan, 2002, p. 4.

[8]Okonkwo argues that the code was modeled closely on the code introduced into the state of Queensland, Australia, in 1899 and which code, in turn, was based mainly on a criminal code drafted by one of the most eminent English criminal law brains, Sir James Fitzstephen in 1878, and proposed to replace the common law but never enacted by the British parliament. The state of Western Australia later adopted the Queensland code (See Okonkwo, *Ibid.*, p. 5).

not have envisaged commission of crimes with the use of computer. Because the only possible *locus* within which crimes could be committed was the physical and temporal one, the makers of the code did not contemplate creating provisions for commission of crimes via cyberspace. Be that as it may, the code provides for general principles of criminal law and creates those old offences which are nevertheless today facilitated by the internet. It is completely oblivious to the offences that emerged with the advent of the internet. For instance, the code provides for the definition[9] and classification[10] of crimes, parties to a crime,[11] and the general principles of criminal liability[12] which may equally be applicable *mutatismutandis* to relevant cybercrimes. It also provides for certain traditional offences that are today aided by the internet such as forgery and personation,[13] stealing,[14] defamation,[15] copyright offences,[16] obscene publications,[17] obtaining by false pretences,[18] and so on. But the code does not provide for offences like phishing, hacking, email scam, cyber-stalking, page jacking, unauthorized access to computer systems and network, salami attacks, and e-mail bombing and spoofing, which are peculiarly and essentially computer-generated. At any rate, none of the above offences, traditional or new, can be fought through the Criminal Code as their elements and modes of commission have radically been altered by the nature of cyberspace.

However that may be, even as the makers of the code did not envisage the cyberspace as a *locus criminis*, they at least anticipated the possibility of a party or parties initiating an act or omission in one jurisdiction and concluding same in another jurisdiction and which act or omission can be an element of an offence, as is very common in commission of some cybercrimes. This is evidenced in the provisions for the application of the code as to offences wholly or partially committed in Nigeria. Section 12 of the code states *inter alia* thus:

> With regard to such offences which are of such a nature that they comprise several elements, if any acts or omissions or events actually occurred, which if they all occurred in Nigeria, would constitute an offence, and any of the acts or omissions or events in Nigeria, although all or some of the other acts or omissions or events which, if they occurred in Nigeria, would be elements of the offence occur elsewhere than in Nigeria; then –

[9]Section 2 of the code defines offence as "an act or omission which renders the person doing the act or making the omission liable to punishment under this Code, or under any Act, or Law". This definition has an extra-territorial effect as it refers to punishments under any other Act of Law including the ones yet to be enacted.

[10]Section 3 of the Code classifies offences into felonies, misdemeanours and simple offences. Cybercrimes can without harm be so 'classified'.

[11]Sections 7, 8, 9 and 10 deal with parties to offences. These include the one who does the act or makes the omission, one who does an act or makes an omission to enable or aid another, one who aids another in actually committing the offence, one who counsels or procures any other person to commit the offence, one who joins in forming a common intention to prosecute an unlawful purpose towards commission of offence, and one who is an accessory after the fact to the offence. There is no reason why this would not be applicable to cybercrime.

[12] See the *Criminal Code*, chapter 5 covering sections 22 to 36.

[13]*Ibid*, chapter 43 to 46.

[14]*Ibid*, chapter 34.

[15]*Ibid*, chapter 33.

[16]*Ibid*, chapter 48.

[17]*Ibid*, chapter 21 A.

[18]*Ibid*, chapter 38.

1). If the act or omission, which in the case of an offence wholly committed in Nigeria would be the initial element of the offence which occurs in Nigeria, the person who does that act or makes that omission is guilty of an offence of the same kind and is liable to the same punishment, as if all the subsequent elements of the offence had occurred in Nigeria; and

2). If that act or omission occurs elsewhere than in Nigeria, and the person who does that act or makes that omission afterwards comes into Nigeria, he is by such coming into Nigeria guilty of an offence of the same kind, and is liable to the same punishment, as if that act or omission had occurred in Nigeria and he had been in Nigeria when it occurred.

Even as this provision did not foresee acts or omissions in respect of elements of cybercrimes, yet with little amendment it would take care of the trans-border or transnational nature of some cybercrimes. After all, one can from far away China, for instance, distribute malicious virus that will have damaging effects in Nigeria, or in far away Australia hack into the email of a person residing in South Africa. It would seem that, in any of these instances, some elements of the offence had taken place in one jurisdiction and other elements completed in another depending of course on the theory of jurisdiction adopted. Besides, the provisions are no less consistent with some need for extradition in deserving cases. Section 12A of the code would in similar manner to section 12 apply *mutatis mutandis* to states of the federation of Nigeria in which some federal laws are domesticated partly due to the complex nature of Nigerian legal system and partly due to the principles of federalism. Moreover, on the basis of the rules on *participles criminis*, provisions of sections 13 and 14 of the code deal with counseling and procuration by one outside Nigeria or a state as the case may be.

Furthermore, other relevant provisions of the code are those contained in chapter 17 that deals with offences relating to posts and telecommunications. Thus, sections 161 to 189 provide for specifically postal and telegrams offences. These include stopping mails, intercepting telegrams or postal matter, tampering with telegrams or postal matter, willful mis-delivery of telegrams or postal matter, obtaining telegrams or postal matter by false pretences, secreting letters and telegrams, fraudulent issue of money order, fraudulent messages respecting money orders, and unlawful franking of letters. Others range from sending dangerous or obscene things by post, retarding delivery of telegrams or postal matter, and obstructing mails, to destroying or damaging letter box, placing injurious substances in or against letter box, defacing post office or letter box, violating secrecy in relation to telegrams or postal matter, and negligently injuring telegraphs. No doubt, the provisions do not consider the fact that most of these offences can now be committed in relation to the computer communications and the use of the internet. Surely, today the use of computers and computer networks has outsmarted the use of post and telegrams. Communications relating to commerce, banking, publication, and even criminal activities, for instance, have found faster and veritable medium in the electronics and the internet. Still, this reality is yet to be accommodated in the Criminal Code.

3. Criminal Procedure Act[19]

Criminal Procedure Act is the adjectival corollary of the Criminal Code. It contains the procedures as to the enforcement of the provisions of the code and other relevant criminal laws. Like the code, its present application is restricted to the old southern Nigeria. The date of its commencement was 1st June 1945, approximately seven decades ago. Arranged in twelve chapters and fifty-three parts, the Act provides for the procedures to be followed from the search or arrest of a suspect or an accused person to the execution of a judgment. Surely, the entire Act enacted, as it were, during the pre-internet era did not contemplate its own application to crimes committed with the aid of computer and the internet. Instances abound from the relevant provisions of the Act as to the illustration of these lacunae.

One important example is in relation to the provision for local inspection during summary trial in deserving cases. Section 295 of the Act, which provides for this does not have in mind the inspection of computer systems, files and programmes which today are important aids for commission of crimes. This is also applicable to all provisions that allow for any form of search of places in relation to relevant offences. Another yawning gap in the Act with regard to the subject matter is on the issue of geographical jurisdiction and place of trial or inquires. Section 64 of the Act provides for a court's assumption of jurisdiction under certain circumstances. The section provides, *inter alia*:

> Subject to the powers of transfer contained in the Act or law constituting any court, the place for the trial or investigation of offences by such court shall be –
>
> (a) an offence shall be tried or inquired into by a court having jurisdiction in the division or district where the offence was committed;
>
> (b) when a person is accused of the commission of any offence by reason of anything which has been done, or of anything which has been omitted to be done, and of any consequence which has ensued, such offence may be tried or inquired into by a court having jurisdiction in the division or district in which any such thing has been done or omitted to be done, or any such consequence has ensued;
>
> (c) when an act is an offence by reason of its relation to any other act which is also an offence, a charge of the first mentioned offence may be tried or inquired into by a court having jurisdiction in the division or district either in which it happened, or in which the offence with which it was so connected happened;
>
> (d) (i) when it is uncertain in which of the several divisions or districts an offence was committed; or
>
> (ii) when an offence is committed partly in one division or district and partly in another; or
>
> (iii) when an offence is a continuing one, and continues to be committed in more divisions or districts than one; or

[19] *Criminal Procedure Act* Cap C 41, L.F.N. 2004 enacted originally as *Criminal Procedure Ordinance* No. 42 of 1945.

(iv) when it consists of several acts committed in different divisions or districts, it may be tried or inquired into by a court having jurisdiction in any of such divisions or districts;

(e) an offence committed while the offender is in the course of performing a journey or voyage may be tried or inquired into by a court in or through or into the division or district of whose jurisdiction the offender or the person against whom or the thing in respect of which the offence was committed resides, is or passed in the course of that journey or voyage;

(f) an offence committed at sea or elsewhere out of Nigeria, which according to law may be tried or inquired into in Nigeria, may subject to the provisions of section 58 of this Act, be so tried or inquired into at any place in Nigeria to which the accused person is first brought, or to which he may be taken thereafter.

There is no doubt that the above paragraphs have delineated the varieties of possibilities or conditions under which courts can assume jurisdictions in respect of offences. Jurisdiction is a very fundamental issue in dispensation of legal justice. Ogbuinya regards jurisdiction as "the linchpin and touchstone of judicial process".[20] Jurisdiction, according to the Halbury's laws of England, means "... the authority which a court has to decide matters that are litigated before it or to take cognizance of matters presented in a formal way for its decision".[21] This illuminating definition of jurisdiction had received at several moments the imprimatur of the Nigeria courts in a myriad of cases.[22] As jurisdiction is germane to litigations in municipal courts, it is no less congenial in matters of adjudication under international jurisprudence.[23] This is because in both municipal and international justice consideration, a court trial or judgement no matter how well conducted or delivered, as the case may be, would be a nullity if the court wrongly assumed jurisdiction.[24]It may be apt to ruminate a bit on the above provisions of the Act with a view to ascertaining their adequacy or otherwise vis-à-vis jurisdictional issues in the fight against cybercriminality in Nigeria today.

The provisions of section 64 of the Act are spread in six paragraphs, namely, (a) to (f). A careful reading would reveal that the first five paragraphs, (a) to (e), concern jurisdictions within a state while the last one, paragraph (f), provides for the possibility of offences committed outside the Nigeria territorial boundaries. While paragraph (a) can *mutatismutandis* apply to cybercrimes that are wholly committed in one division of a High Court or in a Magisterial district, it may however be difficult to determine the particular location where the offence took place. This is due to the essential difference between real space and cyberspace. In the world of cyberspace which exists by way of interconnected networks of computers, one can be in a particular physical locality such as Awka in Anambra State and via a modem powered from a telecommunication company's office in Ikeja in Lagos State, do an act or make an omission

[20]Ogbuinya, O.F., *Understanding the Concept of Jurisdiction in the Nigerian Legal Systems*, (Snaap Press Ltd., Enugu, 2008), p. 1.

[21]Vol. 10, 4th Edition, para 715.

[22] See for instance, *Madukolu v. Nkemdilim* (2006) 2 LC 208 or (1961) NSCC (vol. 2) 374.

[23] *Huntington v. Attrill* (1893) AC 150; *Government of India v. Taylor* (1955) Ac 491; *Attorney-General of New Zealand v. Ortiz* (1982) 3 All E R 432; *Re State of Norway*, Application (1986) 3 W L R, 452; etc.

[24] See *Madukolu v. Nkemdilim*(*supra*).

which results to a cybercrime in Jos, Plateau State. In this event, there arises a problem of which Federal High Court division would have jurisdiction. However, the problem seems to have been laid to rest by paragraph (b) which allows the court situate at where the act was done or omission made, or otherwise, the court where the consequence of the act or the omission was felt, to assume jurisdiction. The difficulty, however, arises if any part of Northern Nigeria is the place of consequence of the act or the omission, in which place the Act does not apply. Even if such provision is in the Criminal Procedure Code which is the Act's adjectival counterpart in the North, there may not be any agreement between the two geographical jurisdictions or even between states for reciprocal enforcement due to the doctrine of territorial application of laws, substantive or procedural.

The study imagines that the scenario painted by paragraph (c) can be illustrated with the real situations of where, for instance, one commits the offence of criminal assault against a person while staying in one division or district, and the victim eventually dies as a result, perhaps in a hospital in another division or district. This is a good representation as criminal assault and manslaughter/murder are both created offences under the Criminal Code.[25] This illustration can also be made of computer crimes. One can, for instance, stay from a room in one division or district and spread computer virus that will be the cause of denial of internet service in another division or district. Paragraph (c) of the Act envisages these kinds of situation and provides that either the court at the place where the first offence was committed or the court where the second offence took place assumes jurisdiction. However, in the case of cybercrimes, the difficulty of determining the place either of the first offence or of the second, or of both offences still persists. Nevertheless, to further belly the jurisdictional ache, paragraph (d) seems to take care of all uncertain situations as to the particular division or district where the offence was committed. The paragraph provides that any of the courts within the scope of relevant or reasonable considerations may try or inquire into the matter in the case of distributed, continuing or divided acts that constitute an offence. This paragraph,which seems to be an omnibus provision is the most preferred in relation to the nature of cybercrime which determination of its actual *locus criminis* is an uphill task. More still, paragraph (e) which contemplates commission of a crime while on a journey or voyage is quite relevant. This is all the more appropriate today where in the case of computer crimes a person may be traveling with a connected personal computer laptop or GSM phone device from or through which the person may do acts or make omissions that may lead to cyber offences. The paragraph covers all possible situations by providing that the court in or through or into the division or district of whose jurisdiction the offender or the person against whom or the thing in respect of which the offence was committed resides, is, or passed in the course of that journey or voyage may try or inquire into the offence. Hence, the victim of the offence may be a person or a thing.

Finally, paragraph (f) is the one that deals with issue of a court's assumption of jurisdiction where the offence in question was committed outside Nigeria or in the High Seas where ordinarily Nigerian courts would not have jurisdiction. This provision specifies that under this dispensation, the court at any place in Nigeria where the accrued person was first brought or to which place he may be taken thereafter may inquire into or try the matter. This provision which contains the clause "subject to section 58" had been repealed by Decree No. 5 of 1967. It then follows that the paragraph would be construed *dehors* the subjection. The beauty of the

[25] See the Criminal Code, Section 252 (assault), section 316 (murder), section 317 (manslaughter).

paragraph's provision lies in its relevance to the transnational or transborder nature of some offences like cybercrimes. Nevertheless, one major problem may arise as to whether the offence sought to be inquired into or tried constitutes an offence in the country from which the accused was brought and if it does whether there is a mutual agreement between Nigeria and that other country as to reciprocal enforcement against the crime.

It is worthwhile to consider the fact that the entire provisions of section 64 are subject to the powers of transfer contained in the Act or law establishing any Act. The implication is that the provisions of section 64 in spite of their strengths or weaknesses are not on firm ground as powers of transfer either in the Act or any other law would prevail at the event of conflict. Section 64A dealing with offence against a federal law is rather more definite. While paragraph (a) covers a situation where an offence is begun in a state and completed in another, paragraph (b) is concerned with where the offence is completed in the state after it was begun in another state. It appears that the combined effects of paragraphs (a) and (b) of the section are tantamount to the fact that an offender may be dealt with, tried or punished as if the offence had been actually or wholly committed in a state, where the expression "a state" can mean both the state where the offence began and the state where it is completed. Further still, by virtue of section 65 of the Act, if the crime is a state offence, a judge has the final decision as to venue within the state in the case of unresolved doubt. Section 67 (1), on the other hand, allows for a remitting of accused person under certain circumstances to another Magistrate. Such circumstances consist in a situation where the accused committed an offence within a magisterial district but was brought to another magisterial district for trial. The law provides that the Magistrate in-charge of the later district should remit the matter to the former unless he was properly authorized to proceed in the case.

Be that as it may, all the provisions of the above sections, namely, sections 64, 65 and 67, regarding place of trial or inquiry are all subject to section 70 of the Act:

> Notwithstanding the provisions of sections 64, 65 and 67 of this Act, a judge or magistrate of a division or district in which is a person is apprehended who is charged with an offence, alleged to have been committed in another division or district, may, if he considers that the ends of justice would be better served by hearing the charge against such person in the division or district in which he has been apprehended and having regard to the accessibility and convenience of the witnesses, proceed to hear the charge, and the person charged may be proceeded against, tried and punished in any division of district in which he was apprehended, or is in custody on a charge for the offence or has appeared in answer to a summons lawfully issued charging the offence as if the offence had been committed in that division or district, and the offence shall, for all purposes incidental to or consequential on the prosecution, trial or punishment thereof, be deemed to have been committed in that division or district.

What is salient in the provision is that the Magistrate at the place of apprehension can assume jurisdiction *in debitojustitiae*, that is, in the interest of justice. The determination of what is in the interest of justice is however left to the whims of his consideration and discretion.

Again, such a Magistrate must also consider the accessibility and the convenience of the witnesses. The proviso to the section also indicates a no mean attention to the relevant even if minimum comfort of the accused. The proviso states:

> Provided that, if at any time during the course of any proceedings taken against any person before any court in pursuance of this subsection it appears to the court that the accused would suffer hardship if he were proceeded against and tried in the division or district aforesaid, the court shall forthwith, but without prejudice to a magistrates power under section 67 of the Act, cease to proceed further in the matter under this subsection.

Section 70 (2) makes provision for a court to assume all jurisdiction to proceed against, try and punish the offender in the case of one charged to it with two or more offences, and deem all the offences charged as committed within the division or district of the court. With respect, this provision is most fluid for at least the singular reason of not indicating that the offences must have been committed on a series of connected acts. Surely, without such qualification, it would not make much sense for a court to assume jurisdiction over offences charged to it irrespective of where they were respectively committed. It would need to be demonstrated that such assumption of jurisdiction is done in the interest of justice as stipulated by section 70 (1). More so, section 71 is most permissive with respect to a court's assumption of jurisdiction after commencement of proceedings even when it is clear that the court should not ordinarily assume such jurisdiction. The section states, *inter alia*, that subsequent to such wrong commencement "all acts performed and all decisions given by the judge or magistrate during the trial or inquiry shall be deemed to be valid in all respects as if the jurisdiction had been assumed prior to the performance of the said acts and the giving of the said decisions".

By and large, one would still need to consider, albeit, briefly what the above provisions of the Act taken together portend for court's jurisdiction to try cyber offences. There is no gainsaying that the original contemplation of the Act with regard to commission of offences is restricted to the *physio-temporal locus*. Thus, such terms as 'divisions' and 'districts', no doubt, refer to real places that are accessible though the physical senses. They are places that can be walked or run on or into with the legs or gone on or into with automobiles and the like. They are places that one can sight and see with the human eyes. They are temporal spaces in which one can touch, hold and smell objects. By 1945 when the Act was enacted, the provisions on jurisdiction and venue of trial and inquiry could not have envisaged the commission of offences through the connected network of computers forming a cyberspace that is quite intangible and incorporeal. Yet the fluidity and the flexibility of the law in the above provisions are an advantage that would allow for an amendment that incorporates considerations for offences in the cyber world. Just a little touch, the law would be tailored to cover the cyber-field.

Section 147 provides for the description of persons in criminal process. Thus, the near anonymity that characterizes cyber offenders seems to find relevance in the provision. It is stated thus:

> Where in any complaint, summons, warrant of any description, charge sheet, information or any document whatsoever issued by a court in

> the exercise of its criminal jurisdiction it is necessary to refer to any person, the description or designation of that person shall be such as is reasonably sufficient to identify him, without necessarily stating his correct name, or his abode, style, degree, or occupation, and if, owing to the name of the person not being known or for any other reason, it is impracticable to give such a description or designation, such description or designation shall be given as is reasonably practicable in the circumstances, or such person may be described as "a person unknown".

Hence, with necessary changes and adaptation, forensic investigations that may track offenders whose addresses and personal details may not fully be known may find recourse for the purpose of prosecution, to the reviewed version of the above provision. This is also all the more possible as section 150 of the Act permits charges to be set out not merely as in the forms in the Second Schedule of the Act but may in the deserving circumstances be modified and adapted in such respects as may be necessary.

However that may be, the author observes that in spite of the wide scale use of computer and the internet system in execution of criminal acts, among other things, it is not definite whether or not a search can be ordered to be carried out on a computer, as provided by section 266 of the Act in respect of specified items therein. The section provides:

> Where a magistrate is satisfied by information on oath that there is a reasonable ground for believing that there is in the state in any building, ship, carriage, receptacle or place anything in respect of which an order may be made under section 264 or 265 of this Act, such magistrate may issue search warrant to search for any such thing and if such thing be found the same shall be brought before any court and dealt with as the court may think proper.

Section 264 referred to provides for the court's power to order for the seizure, forfeiture or confiscation of any instruments, materials or things which there is reason to believe are provided or prepared, or being prepared with a view to the commission of any offence triable by the court. On the other hand, section 265 states the powers of the court upon conviction of the accused to order for the confiscation and destruction of all copies of the things in respect of which the conviction was had and which are in the custody of the court and also those which remain in the possession or power of the person convicted. The conviction referred to by the Act under this section relates to seditions, prohibited or obscene publications and of obscene objects as criminalized by sections 51, 58 and 232 of the Criminal Code. No doubt, today the computer and the internet are an easy medium for the commission of the offences referred to. Yet, it is not clear whether the list of objects or places in respect of which a Magistrate can issue an order for a search as empowered by section 266 of the Act includes computer and networked systems. Even if it includes so, the lack of technical know-how on the part of law enforcement agents and the judicial officers many vitiate the attempt to dispense criminal justice in the relevant cases. This is not to talk of attendant breach of right to privacy of the accused or the convict whose systems may house other files or programmes that are outside the purview of the court's

consideration, if at all the enforcement agents are handed the secret codes that would unlock the often encrypted publications or programmes.

Finally, the Act's provision in section 285 (4) on hearing of witnesses, *inter alia*, may need to be expanded to include the possibility of hearing testimonies of witnesses by video conferencing[26] as a result of the transborder character of most cybercrimes. The Act provides:

> The court shall then proceed to hear the complainant and such witnesses as he may call and such other evidence as he may adduce in support of his complaint, and also to hear the defendant and such witnesses as he may call and such other evidence as he may adduce in his defence and also, if the court thinks fit, to hear such witnesses as the complainant may call in reply if the defendant has called any witnesses or given any evidence.

While the Act refers to hearing the complainant, the defendant and their respective witnesses, the author is only referring to the witnesses as the law does not allow for the absence of the defendants in criminal trials.[27] Surely, video conferencing would be a ready to hand tool for hearing the testimonies of witnesses in the far away beyond the seas. The envisaged difficulties and sophistications that may arise are not however insurmountable as the place from which the witness gives his testimonies as video-focused becomes an extension of the court accessible electronically by the revenant officers and parties. Cross-examination can also follow the same course. This recommendation thus yearns for the amendment of section 354 of the Act that provides for mandatory attendance of witnesses.

All in all, in spite of the loopholes in the Criminal Procedure Act vis-à-vis adjudication over cyber crimes, the Act is not entirely useless in connection therewith. It in fact contains an omnibus provision that heals from the root (*sanatio in radice*) all the inadequacies harboured therein. Section 363 provides that "the procedure and practice for the time being in force of the High Court of Justice in England in criminal trials shall apply to trials in the High Court in so far as this Act has not specifically made provisions therefor". The implication is that with regard to cybercrime trials in the High Courts in Southern Nigeria, recourse can be made to the practice and procedure of the High Courts in England in related cases. This provision at least for the time being can be exploited by activist judges before whom cases of cybercrimes may be prosecuted especially in the face of poverty or paucity of legislation in this connection.

---

[26] See Ekwenze, S.A.M.,*Video Conferencing in International Criminal Arbitration Law and Practice,* (Snaap Press Ltd., Enugu, 2010). Although Ekwenze does not extend the video conferencing practice to criminal procedure, limiting it of course to civil procedure, nay, arbitration practice, yet this study sees no reason why it should not be recommended for taking of testimonies of witnesses that may not easily be reached as a result of distance, especially in the cases of cybercrimes that often beat distance in their perpetration.

[27] Section 281 (1) of the *Criminal Procedure Act.*

4. Conclusion

It can hardly be disputed that, in terms of technological advance, mankind has progressed more tremendously in the last fifty years than in any other period of history. One of the reasons for this rapid development in technology is the internet. The internet today affects every facet of human life irrespective of one's location on the globe. Man's daily activities are affected in form, content and time by the computer. Governments, corporate bodies and individuals all receive the benefits of the information revolution.[28]

The burgeoning of the world of information technology, however, leaves much to be desired. It has opened a floodgate of anti-social and criminal behaviours in ways that would have previously been possible.[29]Computer systems and the internet offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways.[30] The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity.

No doubt, Nigeria has a fair share of this global anti-social and criminal behaviour. Yet, cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols. Specific prevalent computer crimes in Nigeria are spam, fraud, obscene or offensive content, harassment, drug trafficking, hacking, and cyber-terrorism, to say the least. No serious impact has been made by the law enforcement agencies to arrest and prosecute the criminals. Hence, Nigeria is a place where computer has been used to commit all sorts of crimes without prosecution, as there is no specific law on cybercrime. The Nigerian police lack internet policing capability. Nigerian law enforcement agencies are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on internet service site mainly for the purpose of extortion. It is very common for the police to demand bribe from cyber café operators that owns sites where suspicious activities are taking place and look the other way. Cyber criminality is a counterpoint on the dignity of the country as a sovereign nation. It is humiliating and injuriously affecting Nigeria's international image, economy and business, and more importantly the socio-psychological development of the child. However, the many a discussion on cybercrimes in Nigeria points towards the fact that Nigeria is operating on anachronistic legal regime, weakened ethical base, stunted technology platform and digitally illiterate environment that are in urgent need of solution.

It is indeed a truism that the efficiency or effectiveness of any measure is proportional to the degree of its rootedness on an adequate legislative framework. This legislative infrastructure is lacking in Nigeria today. The legal regime of a phenomenon can be traced to two broad sources: the legislature and the judiciary. Perhaps, a third arm is the institutional framework which is the implementing agency that enforces the laws made by various authorities.[31]There is therefore a dire need for adequate legislative framework.There should be a review of all Nigerian

[28] United Nations Commission on Crime Prevention and Criminal Justice, *International Review of Criminal Policy – United Nations Manual on the Prevention and Control of Computer Crime*, Para 2, Eight Congress held at Vienna, April 27th to May 6th, 1999, available online at http://www.uncjin.org/8thpdf. Last visited on 04-02-12.[Hereinafter referred to as U.N. Manual].

[29] U.N. Manual at para. 4.

[30] *Ibid.*

[31] Ashaolu, P. &Oduwole, M., *Policing Cyberspace in Nigeria*, (Lifegate Publishers, Ibadan, 2009), p. 129.

relevant laws, substantive or procedural, in order to reflect the progress in computer technology and the possible abuse thereof especially as it relates to cybercrimes. This is because the growing danger from crimes committed against computers, or against information on computers, is not proportional with the adequacy of the existing laws in Nigeria today. Nigeria needs cyber laws that would govern the country's cyber space and give the nation adequate cyber security measures, the creation of laws that would encourage tougher sentences. Without an effective legal act against cybercrime, the efforts of the government to address the scourge will be a mirage. It is worth mentioning that ever since, efforts are still being made towards enacting an anti-cybercrime law. Recently, the office of the National Security Agency (NSA) prepared a draft Cybersecurity Bill which is still making rounds and taking comments before a final draft is sent to the National Assembly.[32] Perhaps one may be singing a different tune as regards the legal regime of cybercrimes in Nigeria when the law is enacted. But for now, law enforcement agents make do with traditional criminal law enactments to prosecute cybercrimes wherever the acts intersect. Save a special cybercrime procedural law, the existing criminal law procedural practices as contained in the Criminal Procedure Act, Criminal Procedure Code and the Evidence Act, shall apply at the moment to these prosecutions.[33]

Ewelukwalaments that up to six bills dealing with computer misuse and cybercrime had failed to become law in Nigeria.[34] He emphasizes that the non-passage of the bills would affect confidence to enter into business transactions because confidence is usually hinged on trust, and the trust element becomes even more critical where one wants to transact business online due to the faceless nature of the virtual market.Offences like computer hacking, spamming, online identity theft, and ordering goods electronically using skimmed credit or debit cards are yet not punishable under Nigerian law and this is likely to seriously dampen interest in e-commerce. As of now, one needs only to be very careful in entering into online commercial transaction. Some of the protective steps one could take include ensuring the installation of a very good internet security package on one's computer systems, being careful about online offers and deals that appear too good to be true, transacting mainly with companies with known brand names. Others include being careful about companies whose physical business addresses are not stated on their websites, buying goods from websites with secure payment portals, and transacting business with companies based in countries with strong legal provisions for cybercrime, data protection and consumer protection.

[32] This Bill is a response to the issue of inadequacy of Cyberlaws in Nigeria, which I have previously raised severally. (See, for example, Ashaolu and Oduwole, *Policing Cyberspace in Nigeria, Op. cit.)* The Bill was made available for comments and I have since sent my thoughts, hoping it will be more properly drafted. We are eagerly awaiting the future of the Draft, although I believe the Draft needs a wholesale evaluation, which some people are doing a great job on at the moment.

[33] Ashaolu, D."McAsh's Thoughts: Combating Cybercrimes in Nigeria1".Retrieved fromhttps://blogs.law.harvard.edu/mcash/2011/12/24/combatingcybercrimesinnigeria/.Last visited on 19-06-11.

[34] The six bills are the Computer Security and Critical Information Infrastructure Protection Bill 2005 (sponsored by the Executive), the Cyber Security and Data Protection Agency (Establishment, etc) Bill 2008 (sponsored by Hon. BasseyEtim), the Electronic Fraud Prohibition Bill 2008 (sponsored by Senator Ayo Arise), the Nigeria Computer Security and Protection Agency Bill 2009 (another executive bill), the Computer Misuse Bill 2009 (sponsored by Senator Wilson Ake) and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 (sponsored by Hon. AbubakarShehuBunu') (See Nkanga, E." Non- Passage of Cyber Crime Bill Decried". Retrieved from http://www.thisdaylive.com/articles/non-passage-of-cyber-crime-bill-decried/88750/.Last visited on 05-06-11).