



AL-HIKMAH UNIVERSITY JOURNAL OF PRIVATE AND BUSINESS LAW (AUJPBL)

VOLUME 1, No. 1, 2021



**A PUBLICATION OF DEPARTMENT OF PRIVATE AND BUSINESS LAW,
AL-HIKMAH UNIVERSITY, ILORIN, NIGERIA**

GUIDELINES FOR CONTRIBUTORS

Al-Hikmah University Journal of Private & Business Law is an annual peer-reviewed Journal published by Department of Private and Business Law, Faculty of Law, Al-Hikmah University, Ilorin, Nigeria. The Journal hereby calls for well researched Articles in the area of: Corporate Law, Taxation, Arbitration Law, Labour Law, Land and Property Law, Intellectual Property Law, Commercial Law, Law of Banking, Finance and Insurance Law, Tort Law, Litigation Practice and Procedure, Environmental Law, Consumer Protection Law, Administration of Estate Law and other fields of law.

STYLE GUIDELINES

1. Language

The language of the manuscript must be English (British Standards)

2. Title Page

The title page should include name(s), qualification(s) institutional affiliation and current position in the institution, Email address and telephone numbers of the author (s).

3. Length of Paper

- (a) Article: 6000-8000 Words
- (b) Note: 4000-6000 Words
- (c) Comment and Case Review: 2000-4000 Words

The manuscript should be typed on A4 paper, using Microsoft word, Times New Roman, main text should be 1.5 line spacing and font size 12 while foot note should be single line spacing, font size 10 with moderate margins (1 top and bottom and 0.75 left and right).

4. Reference shall be by way of **foot notes**, automatically generated.

5. **Reference Style Format:** Authors must follow the Nigerian Association of Law Teachers (NALT) Uniform Citation Guide-Style of Referencing. The standard British citation method should be adopted.

6. **Abstract:** All submissions must contain abstract of 200-250 words, Key words 4-6, introduction and conclusion

7. **Keywords:** Contributor (s) should provide 4-6 keywords which can be used for indexing purposes

8. Authors should further take note that:

Articles are submitted and accepted on the understanding that exclusive copyright is assigned to Al-Hikmah University Journal of Private and Business Law. Authors are however free to use the materials contained in the papers in other works. Authors have the responsibility to ensure that they do not commit plagiarism thereby infringing on the copyright of others. The views expressed in the Articles are exclusively those of the authors and not the responsibility of the editorial board.

Authors should cross-check and confirm the accuracy of information contained in their papers and should indicate the source(s) of data/view referred to.

9. All manuscripts must be submitted to:

Editor In-Chief,

Al-Hikmah Journal of Private and Business Law,

Faculty of Law,

Al-Hikmah University,

Ilorin, Nigeria.

Prof S.A Bello: shittuabellogmail.com 08033649166

alhikmahjournalofpbl@gmail.com mbayero@alhikmah.edu.ng; 08030516209.

mmla-kadri-abdulsalam@alhikmah.edu.ng 08066188201



AL-HIK
JOU
A

PROF SHITTU A. BELLO

MRS MARYAM BAYERO JIMOH

PROF A. T. SHEHU
CHAIRMAN/DEAN

PROF A. ZUBAIR

ASSOC. PROF H. A. HAMMED

MR A. A. AMINU

MR M. M. SULAIMAN

MRS MUTIAT ABDULSALAM M.

EDITOR-IN-CHIEF

EDITOR

EDITORIAL BOARD

MEMBER

MEMBER

MEMBER

MEMBER

SECRETARY

ADVISORY BOARD

PROF ABIODUN AMUDA KANNIKE, SAN
Kwara State University, Malete-Ilorin, Nigeria

PROF JAMILD. MUJUZI
University of the Western Cape Coast, South Africa

PROF SULAIMAN O. RABIU
Usman Danfodio University, Sokoto, Nigeria

DR TAJUDEEN SANNI, (Senior Researcher Fellow)
Nelson Mandela University, South Africa

PROF HAKEEM IJAIYA
University of Ilorin, Nigeria

PROF SAADAT MUHAMEDED-
Gulu University, Uganda

DR VALENTINE T. MBELI
Kampala International University, Uganda

EDITORIAL COMMENT

Al-Hikmah University Journal of Private and Business Law is a peer review journal published annually by the Department of Private and Business Law, Al-Hikmah University, Ilorin, Nigeria. The journal provides opportunity for academics, researchers, scholars, jurists and legal practitioners to reflect on diverse legal issues of International, Regional, National and Islamic jurisprudence. The journal accepts original and well researched articles in any areas of law and other tropical issues.

This maiden edition features 16 articles on various areas of law such as International Law, Information Technology, Telecommunications, Environmental law, Company Law, Constitutional law, Human Rights, Law of taxation, Banking Law, Islamic, Disputes Resolution in Islamic Jurisprudence, Criminal Law and others.

Only the articles that have scaled through peer review process that were selected for publication. I guarantee that you will find those articles very educative and interesting.

Prof. Shittu A. Bello

Editor-in-Chief

Email: shittuabellogmail.com

Tel: 08033649166

**Any request for further information or clarification
should be directed to**

Mutiat Abdulsalam M.

(08066188201)

Secretary

**AL-HIKMAH UNIVERSITY JOURNAL OF
PRIVATE AND BUSINESS LAW**

TABLE OF CONTENTS

Trans-Borders Crimes and Challenges of Implementation of ECOWAS Protocol on Free Movement of Persons and Goods Dr Hanafi A. Hammed.....	1-14
Effective Management of Nigerian Borders to Contain Banditries in Nigeria Abiola Adekunle Saheed.....	15-27
IPOB Agitation for Self-Determination under International Law and Domestic Criminal Responsibility in Nigeria Shuaib Oniye.....	28-37
Legal Frameworks on Provision of Clean Water: Challenges of Accessing Clean Water in Lockdown during Covid-19 Pandemic in Kwara State Maryam Bayero-Jimoh & Mutiat Abdulsalam-Lakadir.....	38-47
New Law on Unfair Competition under the Federal Competition and Consumer Protection Act, 2019 Ogabi P. E.....	48-60
Piercing of Corporate Veil in the Nigerian and English Legal Systems: A Comparative Appraisal Ahmed Abiodun Muhammed-Mikaaeel	61-75
Examination of the Anti-Avoidance Measures to Counter Tax Treaty Abuse/Shopping Isau Olatunji Ahmed.....	76-89
Examination of Tax Evasion as a Ground for Disqualification in Election Petition Proceedings Akin Olawale Oluwadayisi & Moruf Oluwakayode Mimiko.....	90-99
Legal Framework Regulating Juvenile Correctional Facilities in Nigeria: An Overview Bolaji A. Agoro.....	100-113 *
Examining Laws on Cybercrimes and Internet Policy <i>vis-a-vis</i> Privacy Rights in Nigeria D. A. Ariyoosu.....	114-124
Children Rights and Legal Protection for Young Persons under the Nigerian Law: An Appraisal Dr Aderonke Abimbola Ojo & Tosin Ezekiel Ayo.....	125-138

TABLE OF CONTENTS

Effects of the Central Bank of Nigeria Regulatory and Supervisory Framework on Microfinance Banking in Nigeria Fatima Abubakar Nahuche* & Shamsu Yahaya:.....	139-150
Legal Approach in Combating Kidnapping in the Nigerian Upstream Petroleum Industry Dr. Olujobi Olusola Joshua*¹	151-166
Corporate Governance in Nigeria: An Analysis of Nigerian Code of Corporate Governance, 2018 Prof. Shittu A. Bello.....	167-179
Role of Judge and the Constraints of the Executive in the Administration of Justice in Nigeria Prof A. Toriola Ajagbe & Ademola A. Aminu.....	180- 191
Examining The Role Of Legal Aid In The Effective Dispensation Of Justice In Nigeria Azeez O. Kabir Esq.....	192-204

Examining Laws on Cybercrimes and Internet Policy *vis-a-vis* Privacy Rights in Nigeria

D. A. Ariyoosu*

Abstract

The world has truly become a global village as a result of technological developments that have engendered a great advancement in Information and Communications Technology. The virtual world has, in no small amount, contributed to the development of not only the developed world but also the developing and underdeveloped countries. The development has positively touched virtually all aspects of human endeavours – politics, economy, religion, culture and governance. Nigeria as a developing country is left out in this respect. Unfortunately, much as technological advancement has contributed immensely to the economic developments, it has equally brought with it a lot of vices which have confusingly whittled down the effects of these developments as a lot of crimes are being committed over the internet. The objective of this paper is, therefore, to examine the legal regulation of cybercrimes with particular reference to internet policy and privacy rights in Nigeria with a view to addressing and analyzing the extent of crimes being committed over the cyber space. Both primary and secondary sources of law are employed in arriving at a logical conclusion in the research. It has been found that cybercrimes are on the increase and its rampancy is prominent among the youths. It is therefore recommended that in policy formulation, the government should put in place more policies that will be easily executable in determining, apprehending and prosecuting cybercrimes perpetrators.

Keywords: Legal Regulation, Cybercrimes, Internet Policy, Privacy Rights

1. Introduction

The Information and Communication Technology (ICT) revolution has had impacts on almost all areas of human endeavours. From business, industry and government to non-profit organisation, ICT has simplified business processes such as sorting, summarising, coding, editing, customized and generic report generation in a real time processing mode. However, ICT has also brought unintended consequences such as criminal activities, spamming, credit card frauds, Automated Teller Machine (ATM) frauds, phishing, identity theft and other related cyber-crimes.¹

Nigeria as a Country currently lies third globally in cybercrimes just behind the United Kingdom and the United States. The number of internet users in Nigeria is about 91.6 million and the estimated loss to cyber-crime in Nigeria was estimated to be about 127 Billion Naira.²

The internet is a good place to be but unfortunately, there have been unintended consequences through the usage of the internet. This paper tends to examine the Cyber laws and Cyber-crimes vis-à-vis right to privacy and internet policy in Nigeria as well as the usage of internet as a tool for national development.

*LL.B, LL.M, Ph.D, BL, PGDE, ACTI, ACI Arb, AILEX, ACILR, Notary Public, Lecturer, Department of Business Law, Faculty of Law, University of Ilorin, Ilorin, Nigeria. E-mail: ariyoosu4law@yahoo.com; ariyoosu4law@gmail.com. Phone No+2348066497298; +2348185356311.

¹ Wada F and Odulaja G. O., 'Assessing Cybercrime and its Impact on E-Banking in Nigeria Using Social Theories' (2007) 4 (3) Issue 2 *Afr J Comp & ICT*, 69.

² NCC, 'Nigeria Ranks 3rd in Global Internet Crimes behind UK, U.S.'

<<https://www.google.com.ng/amp/s/www.premiumtimesng.com/news/top-news/241160-nigeria-ranks-3rd-global-internet-crimes-behind-uk-u-s-ncc.html/amp>>accessed 01 May, 2018.

2. Definition of Terms

The word "Cyber" is a prefix used to describe an idea as part of the computer and information age. "Crime can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive."³ Cybercrimes had also been defined as "Offences that are committed against individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication network such as Internet (Chat rooms, e-mails, notice boards and groups) and mobile phones."⁴ The term cybercrime was coined by Peter Cassidy, Secretary General of the Anti-Phishing Working Group, to distinguish computer programmes (and coordinated, interlocking sets of programmes) that are designed specifically to animate financial crime from other kinds of malevolent packages.⁵

"Cyber laws" are laws and regulations guiding the usage of the cyberspace. Generally, these laws either restrict and/or guide the usage of social media.

"Internet" may be defined as a global computer network providing a variety of information communication facilities, consisting of interconnected networks using standardised communication protocols.⁶

Privacy rights may be defined as the right of people to live their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbour's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera; and in statutory law, the right of people to be free from unwarranted drug testing and *Electronic Surveillance*.⁷

3. Cybercrimes in Nigeria: Legal Regulation

Cybercrime is a worldwide problem that is costing countries of the world billions of dollars. With the advent of the Internet, cybercrimes have been on the increase. Cyber Law and Regulations have therefore become emerging fields in various jurisdictions.⁸ Cyber Law apparently encompasses cybercrimes, electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law, and privacy rights.⁹ Cybercrimes have continued to pose many challenges to electronic commerce and have rendered internet business vulnerable to manipulation by persons who are not parties to a transaction. Cyber criminals have, over the years, adopted series of innovative strategies to induce and trap the internet users into carefully designed schemes that are more stealthy and sophisticated than ever before.¹⁰ As a result, many hackers

³ Anah B H, Funmi D L and Julius M, 'Cybercrime in Nigeria: Causes, Effects and the Way Out,' (2012) 2 (7) *African Journal of Science and Technology*. 626.

⁴ Halder D and Jaishankar K, 'Cybercrime and the Victimization of Women: Laws, Rights and Regulations,' (2012) Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

⁵ Herselman M and Warren M, 'Cyber Crime Influencing Businesses in South Africa', (2003) 1 *Journal of Information Science and Information Technology*, 253.

⁶ Internet <<https://www.google.com/search?q=definition+of+internet&ie=utf-8&oe=utf-8&client=firefox-b>> accessed 02 May, 2018.

⁷ <<https://legal-dictionary.thefreedictionary.com/Privacy+rights>> accessed 02 May, 2018.

⁸ For instance, there is UK Computer Misuse Act 1990; UK Terrorism Act 2000, which came into force on 19 February 2001 and amended by the Anti-terrorism, Crime and Security Act, 2001; Information Technology Act 2000 of India; UK Data Protection Act 1998; US Electronic Transactions Act 1999; US Uniform Computer Information Transactions Act; US Paperwork Elimination Act 2001; UNCITRAL Model Law on Electronic Signatures 1998; European Union Directive 97/66/EC of the European Parliament and of the Council of 15 December, 1997; European Union Directive 99/93/EC of the European Parliament and of the Council; European Union Directive 2000/31/EC of the European Parliament and of the Council.

⁹ See Rodney D. R, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and Internet)* p.1068.

¹⁰ Vivek S, *Cyber Crimes, Electronic Evidence and Investigation Legal Issues* (Nabhi Publications, New Delhi, India 2008) 63.

other cyber criminals can flourish in countries with few Internet crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as the internet has no geographical demarcation.¹¹ In Nigeria, cybercrimes are performed and carried out by people of all ages, ranging from young to old, but in most instances, the young. Several youths engage cybercrimes to boost their ego, or as a profit-making venture since the tools for hacking in our modern world have become affordable by many.¹²

Unfortunately, it has been held that the probable way of proving the commission of internet crimes is circumstantial evidence as the crime can even be committed right inside the culprit's room. Thus, In the Court of Appeal case of *Harrison Odiawa v Federal Republic of Nigeria*,¹³ Dongban-Mensem JCA held that the nature of internet crimes and the extent of circumstantial evidence as the plausible means of discovering exploiters of Information Technology in the commission of crime as follows:

The crime which colloquially has come to be known as "419" and the constitutive term of which is not known as advanced fee fraud is a well-premeditated crime. It is like the crime of armed robbery. The only difference here is the words. The internet, letters and telephone, are the "arms" rather than "guns" and other lethal weapons. The criminal can commit his crime in the comfort of his bedroom.

The common feature of the two crimes are the planning and executions; like the armed robbers who sometimes use masks, with internet robbery, the perpetrators, employ all sorts of gimmicks to cover up their trails. The point one strains to make here is that circumstantial evidence is the only plausible if not probable means of discovering the true monsters and exploiters of the I. T. (Information Technology) in the commission of crime. This is until the same I. T. creates some definite means of detection. Nigeria, like several other countries, has laws regulating Cybercrime and usage of cyberspace generally. These laws shall be discussed in the following paragraphs.

• The Cybercrime Act, 2015

The Cybercrime (Prohibition, Prevention, etc) Act, 2015 is one of the viable laws regulating Cyberspace in Nigeria. The Act provides an effective, unified and comprehensive legal regulator and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It criminalises many of the wrongful acts being executed on the internet. According to the Act, any unauthorised modification of computer data is a crime punishable with three years imprisonment or an option of fine of not more than ₦7,000,000.00 only or both fine and imprisonment¹⁴ while any person who engages in damaging, deleting, deteriorating, altering, restricting or suppressing data within computer systems or networks is also liable upon conviction to a minimum of two years imprisonment or a fine of not more than ₦5,000,000.00 or both fine and imprisonment.¹⁵

The Act also prohibits unlawful system interference and a person where convicted for such is liable to a minimum of two years imprisonment or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.¹⁶

¹¹ Guillaume LF, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges' *Virus Bulletin Conference* (2009).

¹² *Ibid.*

¹³ (2008) All FWLR (Pt 439) 436.

¹⁴ Cybercrime Act, 2015, s. 16 (1).

¹⁵ *Ibid.*, s. 16 (3).

¹⁶ *Ibid.*, s. 8.

The Act also prohibits the misuse of devices and any person charged with same is liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.¹⁷

The Cybercrime Act also provides for offences of Computer related fraud and persons charged with same are liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.¹⁸ The offence of identity theft is also punishable with imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.¹⁹ It also include the offence of cyber stalking punishable with imprisonment for a term of not less than one year or a fine of not less than N2,000,000.00 or to both fine and imprisonment.²⁰ The Act prescribes a punishment of life imprisonment for any person convicted of the offence of Cyber terrorism.²¹

It is pertinent to also point out that the business of cyber café or cyber business must be duly registered. Thus, all cyber café operators are duty bound to register as a business concern with Computer Professionals Registration Council in addition to a business name registration with the Corporate Affairs Commission, and maintain a register of users through a sign-in register, which shall be made available to law enforcement personnel when needed.²² The implication of this is that the section makes it easy to track perpetrator of online fraud, as the register will serve as a database of all persons who have used the internet service provided by the Internet Service Provider in question in any given cyber café. The Act makes it an offence for any person who perpetrates electronic fraud or online fraud using a cybercafé and such a person shall be liable on conviction to a fine or term of imprisonment or both.²³ and if it is proved that there was connivance by the cyber café owners, the latter will be guilty of an offence and liable on conviction to a fine or three years imprisonment.²⁴ The burden of proving connivance by the owner of the cybercafé is, however, on the prosecutor.²⁵

The Nigeria Criminal Code Act

The Criminal Code Act²⁶ criminalises any type of stealing of funds in whatever form, and makes such offences punishable. Although, cybercrime is not specifically mentioned in the Act, it is a type of stealing punishable under the Criminal Code. The most relevant provision of the Act is Chapter 38 dealing with "Obtaining Property by false pretences; Cheating" and spans Sections 418-426 of the Act. Several provisions of the Act frown at cybercrimes and the most relevant of them will be mentioned here.

Section 418 provides thus:

"Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence."

¹⁷ s. 8.

¹⁸ s. 14.

¹⁹ s. 13.

²⁰ s. 24.

²¹ s. 18.

²² s. 7 (1).

²³ s. 7 (2).

²⁴ s. 7 (3).

²⁵ s. 7 (4).

Section 419 provides thus:

Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

Section 383(1) of the Act states:

A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing.

The effects of the above quoted provisions of the Act is that where the act complained of is committed as a result of false representation, false pretences or fraudulent conversion of anything capable of being stolen through the internet, then offences in those sections are deemed to have been committed.

It should be noted that the Criminal Code is applicable in the Southern States of the Federation while its counterpart Penal Code is applicable in the Northern States. However, by the coming into effect of the Administration of Criminal Justice Act, 2015,²⁷ the Criminal Procedure Act²⁸ has been repealed while the Criminal Code Laws of the various states in the South are still in operation. Meanwhile, some states of the Federation have enacted their respective Administration of Criminal Justice Law.²⁹

• **Advance Fee Fraud and other Fraud Related Offences Act, 2006**

Section 1 of the Act³⁰ provides that:

1. Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud –
 - (a) obtains, from any other person, in Nigeria or in any other country, for himself or any other person; or
 - (b) induces any other person, in Nigeria or in any other country, to deliver to any person, any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.
2. A person who by false pretence, and with intent to defraud, induces any other person in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act
3. A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than twenty years and not less than seven years without the option of a fine.

Section 20 of the Act defines false pretence as 'a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' The implication of this is that, where the false representation is made by the use of cyberspace, then the representor is guilty of an offence under the Act.

• **The Economic and Financial Crimes Commission (Establishment) ACT, 2004³¹**

Economic and financial crime has been defined as:

²⁷ The Administration of Criminal Justice Act, 2015, s. 439.

²⁸ Cap C41, Laws of the Federation of Nigeria, 2004.

²⁹ For instance, Administration of Criminal Justice Law of Lagos State, 2007 (Re-enacted in 2011), Administration of Criminal Justice Law of Oyo State, 2016, Administration of Criminal Justice of Kaduna State, 2017 and Administration of Criminal Justice of Anambra State, 2010.

³⁰ Which is now embodied in the updated Cap. A6, Laws of the Federation of Nigeria, 2010

³¹ Now embodied in Cap E1, Laws of the Federation of Nigeria.

the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labor, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods etc.³²

It does not matter whether any of the above acts constituting the offence under the Act is done physically or virtually by the use of the internet. Once it is done, the offence is deemed to have been committed.

4. Classification of Cybercrime

Cybercrime has been classified into three. They include:

1. Cybercrime against persons
2. Cybercrime against property
3. Cybercrime against Government

Cybercrime against persons refers to the crime committed against persons through the usage of the internet. They include cyber bullying, trafficking, intimidation and harassment, distribution of obscene materials like pornography and indecent pictures without authorization, stalking, hacking and cracking of websites mails and many others.³³

Cybercrime against property refers to the crime against property through the use of the cyberspace or the internet. They include theft of intellectual property, internet fraud, transmission of viruses and malware to others devices and many others.³⁴

Cybercrime against the Government includes crimes committed against the State/Government through the use of the internet. They include cyber terrorism, theft of military hardware, hacking and cracking of Government websites and many others.³⁵

5. Types of Cybercrime

Various types of cybercrimes have been identified and these include computer sabotage, hacking, unauthorised copying of computer programs, cyber fraud, cyber stalking, phishing, data and Information theft, criminal intimidation, outraging the modesty of women and violation of privacy.³⁶ Some of the types of cybercrimes shall be briefly examined:

• Fraud

Cyber Fraud, such as phishing³⁷ and identity theft, has become very rampant. Organised crimes have used cyber space to target credit card information, personal and financial information for computer fraud. The sale of this information to counter-feiters of credit cards has proved to be extremely profitable and the issue of stealing of bank or credit cards is no longer of moment to the fraudsters. The phishing, in most cases, is

³² Economic and Financial Crimes Commission (Establishment) Act 2004, s. 46.

³³ Shambhavi T., 'Cyber Crimes: Classification and Cyber Forensics' <<https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics/>> accessed 02 May 2018.

³⁴ Ibid.

³⁵ Ibid.

³⁶ See generally, the United Nations Manual on the Prevention and Control of Computer-Related Crime. See also Vivek Sood, *Cyber Crimes, Electronic Evidence and Investigation, Legal Issues* (Nabhi Publications, New Delhi, India, 2008) 68-108 and Rodney D. R., *Guide to Cyber Laws (Information Technology Act, 2000, Ecommerce, Data Protection & the Internet)*, (3rd Ed, Wadhwa and Company Law Publisher, New Delhi, India, 2007) 1076-1079.

³⁷ Phishing means impersonation of a trusted entity on the internet, to dishonestly and fraudulently induce the victim to provide information. It is the wrongful obtaining of data by impersonation. It suffices to say therefore that impersonation is the core of phishing.

the preparation or in other words, the first step towards committing cheating, misappropriation or forgery. The personal information that is fraudulently obtained is misused to commit these crimes. Automated Teller Machine (ATM) fraud has been on the increase as a result of phishing.³⁸ The form of electronic fraud would determine the legal approach to be adopted in combating internet fraud.

- **Forgery**

Computer Forgery is the alteration of computerised documents. A new generation of fraudulent counterfeiting has emerged as a result of the advent of high-resolution computerised colour laser copiers and these copiers can modify existing documents, the quality of which is indistinguishable from the original. The evidential value of these documents may not really become an issue unless and until it is discovered that the documents are not original but counterfeit, and this may only be discovered by referring to an expert for analysis where forgery is noticeable *ex facie* the documents.³⁹

- **Computer Sabotage/ Malware**

Computer Sabotage is the use of the internet to hinder the normal functioning of a computer system through the introduction of computer contaminants and viruses.⁴⁰ It has been observed that every computer would suffer from a computer virus at some point in time or other and the viruses get into computer through a Compact Disc (CD) Floppy or pen-drive that is corrupted or through the internet.⁴¹ Computer Sabotage can be used to gain economic advantage over a competitor, to promote illegal activities of terrorists, or to steal data or programme for extortion purposes.⁴² Thus, people need to be aware of the emergence and existence of computer contaminants and viruses with a view to being equipped with strong anti-virus software and know how to use it.

- **Cyber Stalking**

Cyber Stalking refers to the activity of users sending harassing or threatening e-mail to other users. Stalking causes nuisance and beyond a certain point it becomes harassment. The content of cyber stalking is mostly harmless but the repetitiveness of the act creates nuisance, irritation and harassment. This can also be called Cyber bullying.⁴³

- **Hacking**

Hacking a computer is an unauthorised access to a computer system or services. It could be for the purpose of sabotaging the computer system. Hacking a computer simply implies gaining unlawful access to another's computer. It is equivalent to phone tapping. Hackers frequently impersonate the system

³⁸ See the following cases where the issue of ATM fraud arose and the claimants succeeded in their respective claim for the refund of the money withdrawn through ATM without their authorisation: *Kingsley Chigozie Nnawuba v UBA* (Unreported) Suit No. LD/1116/2008 of 27 May 2011 delivered by Jose J; *Ibrahim Quadri v. Guaranty Trust Bank Plc* (Unreported) Suit No. KWS/189/2010 of 22 November 2010 delivered by A. O. Bamigbola J.

³⁹ Rodney D. R., *Guide to Cyber Laws (Information Technology Act, 2000, Ecommerce, Data Protection & the Internet)* 1076-1077.

⁴⁰ Computer contaminants include worms and logic bombs. A worm is designed to alter or destroy data but it lacks the ability to replicate itself, while a logic bomb or time bomb is a program that is written to modify or destroy data at a specific date and time in the future. A virus is a program that has the ability to attach itself to legitimate programs and to replicate and attach itself to other computer programs. See generally Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 1077. See also Gringras C., *The Law of the Internet* (2nd ed, Butterworths LexisNexis, London, 2008) 303-304.

⁴¹ Vivek Sood, *Cyber Crimes Electronic Evidence and Investigation, Legal Issues* (Nabhi Publications, New Delhi, India, 2008) 83.

⁴² Rodney D. R., *Guide to Cyber Laws (Information Technology Act, 2000, Ecommerce, Data Protection & the Internet)* 1077.

⁴³ *Ibid*, 1078-1079.

administrator, using default maintenance passwords, which the real system administrator failed to change, to break into the system.⁴⁴ The modern hackers can by-pass existing system password protection by creating a Trojan horse programme to capture the password of legitimate users of the system.⁴⁵ Hacking is considered one of the most serious of all cybercrimes as it is said that hacking erodes the faith of the people in information technology and the internet.

Unauthorised Copying and Distribution of Computer Programme

The unauthorised copying and distribution of computer programme can cause considerable economic loss to the legitimate owners. This activity has been held to be criminal in nature and subject to criminal sanctions. In *U.S. v David Lamachia*,⁴⁶ the court ruled that criminal and civil penalties should attach to defendants involved in willful and multiple infringements of copyrighted software even if the infringer lacked commercial motive. Business Secret, technical know-how, designs, music, films, books and personal data are some forms of intellectual property that drive the information economy and are valuable. This is an area where infringement of Intellectual Property comes in because of the money, time, efforts and creativity expended in creating the work of intellectual property.

Cyber Terrorism

is an act of terrorism committed through the use of internet. A cyber terrorist can be described as someone who launches attack on government or organisation in order to distort and or access stored information on the computer and their networks.⁴⁷

Spam/Phishing

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognised form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki pages, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.⁴⁸ Phishing is not only a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing.⁴⁹

Cyber Law and the Right to Privacy

Prosser⁵⁰ argues that: It would be a good thing if privacy could be protected, but the war and way of technology and the needs of security have *de facto* made the right to privacy a dead letter.⁵¹ The right to privacy and family life of every Nigerian is enshrined in section 37 of the Nigerian 1999 Constitution (as amended). The abovementioned section provides thus: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'

⁴⁴ Ibid, 1078.

⁴⁵ Ibid.

⁴⁶ Crim. A. No. 94-10092-RGS, US Dist. (D. Mass. Dec. 28, 1994) cited in Rodney D. Ryder, *Guide to Cyber Laws and Information Technology Act, 2000, E-commerce, Data Protection & the Internet* 1078.

⁴⁷ Dlusola M. and Samson O., 'Cyber Crimes and Cyber Laws in Nigeria' *The International Journal of Engineering Science (IJES)*, (2013) 2 (4) 19-25.

⁴⁸ Ibid, 21.

⁴⁹ Wada & G.O. Odulaja, *Assessing Cybercrime and its Limit on E-Banking in Nigeria Using Social Media Theory*

⁵⁰ Miller J. M., 'Dignity as a New Framework, Replacing the Right to Privacy' 30 T. Jefferson L. Rev. 1 [2007-2008] 1.

⁵¹ Ibid.

The African Charter on Human and Peoples' Rights⁵² duly guaranteed the Right to privacy of Africans in its Article 18 which provides thus: 'The family shall be the natural unit and basis of society. It shall be protected by the State which shall take care of its physical health and morals.'

Article 12 of the Universal Declaration of Human Rights 1948 also provides as follows: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

Generally, an invasion of private or family life by a person or public authority may entitle the individual whose right was infringed upon to sue for trespass, defamation or other tort as well as crime.

Thus, illegal hacking and cracking of mails, websites, social media accounts, posting of unauthorised pictures of persons on the internet, stalking, and many others are infringement on the rights to private or family life of fellow Nigerians which is actionable. However, the right to private family life like every other constitutional rights has limitations which is provided under Section 45 (1) (a) and (b) of the Nigerian 1999 Constitution (as altered). The limitations include any law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health; for the purpose of protecting the rights and freedom of other persons or through emergency situations.⁵³

Article 27(2) of the African Charter on Human and People's Right also provide for a limitation to the various rights provided in the charter, the right to Private Family Life inclusive. It provides thus: The rights and freedom of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest.

7. Data Privacy Protection in Nigeria

As it has been discussed above, the Right to privacy of Nigerians is sacrosanct and same must be adequately protected. One of the major data protection policies could be found in the Consumer Code of Practice Regulations 2007 (NCC Regulations) issued by the Nigerian Communications Commission (NCC); the governing body for all telecommunications companies in Nigeria. The Regulations provide that all licensees must take reasonable steps to protect customer information against 'improper or accidental disclosure' and must ensure that such information is securely stored. It also provides that customer information must 'not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations'.⁵⁴

The National Information Technology Development Agency (NITDA) which is the agency responsible for planning, developing and promoting the use of information technology in Nigeria also issued guidelines on data protection known as the "NITDA Guidelines". The NITDA Guidelines prescribes the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information and is currently the only set of regulations that contains specific and detailed provisions on the protection, storage, transfer or treatment of personal data.⁵⁵

⁵² African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, *Cap A9 Laws of the Federation of Nigeria 2004*.

⁵³ *FRN v Daniel* (2011) LPELR-4152.

⁵⁴ Consumer Code of Practice Regulations 2007, ss. 43 & 44. See also <<https://www.ncc.gov.ng/documents/780-consumer-code-of-practice-regulations-2018/file>> accessed 02 May, 2018.

⁵⁵ National Information of Technology Development Agency Data Protection Guidelines 2017, s 6. See also <<http://nitda.gov.ng/wp-content/uploads/2018/02/DATA-PROTECTION-GUIDELINES-Reviewed..pdf>> accessed 02 May, 2018.

The NITDA Guidelines apply to Federal, State and Local Government Agencies and institutions as well as private sector organisations that own, use or deploy information systems of the Federal Republic of Nigeria, and also apply to organizations based outside Nigeria if such organizations process personal data of Nigerian residents.⁵⁶

8. Internet as a Tool of Globalisation

The information technology revolution associated with the internet has brought about two edge functions: that is on one hand, it has contributed positive values to the world; while on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world.⁵⁷

Nigeria as a Country is a nation currently threatened by her youths' unintelligent use of the internet. All the Cybercrimes discussed briefly above and many others are constantly carried out by Nigerian youths. This is not to say that majority of Nigerian youths are not doing well. Notwithstanding, numerous of these crimes still occur all over the country. However, despite several ills that could be brought about by the internet, it has so many advantages if put to proper usage.

One of the many developments that the internet can bring about is the development in the educational sector. The very origin of the Internet is strongly linked to education, as it was in universities and research institutes that electronic networks were initially developed. Such networks have since evolved from the sharing of research findings among scientists and scholars to access to libraries, schools, and universities worldwide. The Internet also enables alternative teaching methods through virtual classrooms and long-distance education, thus allowing more people to receive education.⁵⁸

The ease with which information can be published and disseminated on the Internet allows for more democratic and participatory political structures. For example, referendum, opinion polls and many others can be conducted online without any stress and unusual delay. In many countries of the world, elections are now done online. In fact, several universities in Nigeria now do online advertisement, admission processes and registration of students. Also, an impressive development has been derived in the health sector. Computerised networks facilitate access to accurate and up-to-date information, enable long-distance training and consultation and improve the administration of the health sector. Online initiatives addressing health and medicine promote networking among hospitals and health professionals worldwide and provide updates on current medical research.⁵⁹

The internet is also a major way of ensuring the passage of information within and outside the Country with several media outlets and major newspapers now willing to furnish information online without the need to proceed to the newspaper stand to read the papers. Also, videos and even radio stations can now be streamed online through the use of phones and other devices. These are major developments in Nigeria through the use of the internet.⁶⁰

Conclusion

As demonstrated in this paper, the cyberspace is a double-edged sword. It could be used to bring about development and it could also be used to destabilise the country and also infringe on the rights of fellow

id.

Assan A.B., Lass F.D & Makinde, J. 'Cybercrime in Nigeria: Causes, Effects and the Way Out', (2012) 2 (7) *ARPJN Journal of Science and Technology*.

Paula U., 'The Internet as a Tool for Social Development' https://www.isoc.org/INET97/proceedings/G4/G4_1.HTM accessed 02 May, 2018.

id.

id.

countrymen. Either of the option taken depends on the policies, strategies and regulatory framework place by the Government and the willingness to execute them properly. It is therefore recommended the promulgation of laws and formulation of policies on the use of cyber space, the government should focus on easy ways of determining, apprehending and prosecuting cyber criminals. Thus, the various on IT and other internet related Bills, such as Electronic Transaction Bill, need to be passed into laws

AL-HIKMAH UNIVERSITY
JOURNAL OF PRIVATE
LAW AND BUSINESS
ISSUE 1, NO. 1, 2007

