Cybercrime in Nigeria: An Overview of Laws and Ethics from the Information Technology (IT) Professional's Perspective

[1,2]Dunmade, A.O., [2]Tomori, A.R. & [3]Olatunbosun-Adedayo, A.
[1] Department of Library and Information Science, Adeleke University, Ede, Osun State, Nigeria
[2] Computer Services and Information Technology (COMSIT) Directorate, University of Ilorin, Nigeria
[3] Magistrate Court 1, Ebute Metta, Lagos State, Nigeria
E-emails: derindunmade@gmail.com, derin_d@unilorin.edu.ng,
Phone: +2348032515609

ABSTRACT

The Information Technology Profession is a service-geared profession which covers a wide spectrum of careers. As with all professions in the world it has a well-defined code of conduct which it expects its members to obey, and is binding on all, geared towards honesty, fairness, excellence and impeccable character. The extant laws of the Federal Republic of Nigeria (and indeed all countries) are drawn based on the inbuilt ethos of the human race – that innate expectation that leads us to desire to morally choose good always over evil in every facet of human endeavour. This paper aims to overview the laws of Nigeria – especially the Cybercrime Act of 2015 and the code of conduct of the IT profession with a view to assessing their effect on conforming members of the profession to higher ideals. Recommendations both for IT Practitioners and the general public are made.

Keywords: Cybercrime, Nigeria, Information Technology Practice, Professional Ethics and Conduct

iSTEAMS Multidisciplinary Conference Proceedings Reference Format
Dunmade, A.O., Tomori, A.R. & Olatunbosun-Adedayo, A. (2019): Cybercrime In Nigeria: An Overview of Laws and Ethics from the Information Technology (IT) Professional's Perspective. Proceedings of the 22nd iSTEAMS Multidisciplinary SPRING Conference. Aurora Conference centre, Osogbo, Nigeria. 17th – 19th December, 2019. Pp 13-20.
www.isteams.net/spring2019. DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V22N1P2

1. INTRODUCTION

1.1 Definition of Law

The law is described as the set of statutes, rules and regulations, created by the government in a bid to preside over the entire society. It is universally accepted, recognized and enforced and created with the purpose of maintaining social order, peace, justice in the society and to provide protection to the general public and safeguard their interest. It is made after considering ethical principles and moral values. Laws are made by the legistature of a country and implemented and enforced by the judiciary. Every person in the country is bound to follow the law. It clearly defines what a person must or must not do. Breach of law may result in punishment or penalty or sometimes both.

1.2 Definition of Ethics

By ethics, we mean that branch of moral philosophy that guides people about what is good or bad. It is a collection of fundamental concepts and principles of an ideal human character. The principles help us in making decisions regarding what is right or wrong. Foote (2004) informs about how to act in a particular situation and make a judgment to make better choices for ourselves. Ethics are the code of conduct agreed and adopted by

the people. It also sets a standard of how a person should live and interact with others. He also opines that both the law, ethical beliefs and a professional code of conduct play a joint role in enforcing compliance on those people they oversee.

1.3 Key Differences between Law and Ethics

The major differences between law and ethics are mentioned below:

1. The law is defined as the systematic body of rules that governs the whole society and the actions of its individual members. Ethics means the science of a standard human conduct.
2. The law consists of a set of rules and regulations, whereas ethics comprises of guidelines and principles that inform people about how to live or how to behave in a particular situation.
3. The law is created by the Government, which may be local, regional, national or international. On the other hand, ethics are governed by an individual, legal or professional norms, i.e. workplace ethics, environmental ethics and so on.
4. The law is expressed in the constitution in a written form. As opposed to ethics, it cannot be found in writing form.
5. The breach of law may result in punishment or penalty, or both which is not in the case of breach of ethics.
6. The objective of the law is to maintain social order and peace within the nation and protection to all the citizens. Unlike, ethics that are the code of conduct that helps a person to decide what is right or wrong and how to act.
7. The law creates a legal binding, but ethics has no such binding on the people.

2. INFORMATION AND COMMUNICATIONS TECHNOLOGY AND THE INTERNET

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, Information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings, electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.

Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies and the falling price of computer systems, many more people in developing countries should have easier access to the Internet and related products and services. The influence of ICTs on society goes far beyond establishing basic information infrastructure.

The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

2.1 The IT profession in Nigeria

The Computer Professional's Registration Council of Nigeria (CPN) is an agency of the Federal Government of Nigeria. It is a legal entity charged with the control and supervision of the Computing Profession in the country. It was established to set and enforce the standards of competences, conduct and ethical practice for the Nigerian Information Technology Profession. The Council was established by the Computer Professional (Registration Council of Nigeria) Decree 1993, promulgated as Decree No. 49 on June 10, 1993. It defines the IT professional as that individual who makes use of computational machinery and techniques related thereto on the public, employees and clients.

2.2 The Code of Ethics of the Information Technology Profession in Nigeria

The Code of Ethics of the profession is as stated below:
I acknowledge that I have an obligation to:

1) The public, therefore I shall have utmost regard for its safety, health, and well-being
2) My employer or client whose trust I hold, therefore, I shall serve him faithfully and loyally, endeavouring to discharge this obligation to the best of my ability, guarding his interest and advising him wisely and honestly.
3) Fellow members of the Profession, therefore I shall uphold the ideals of the Profession cooperating with fellow members and treating them with honesty and respect at all times.
4) The Profession, therefore I shall acquire, maintain and improve professional competence, promote the advancement of Computer Science as well as the understanding, effective and efficacious deployment of computational machinery, computerized machinery and techniques related thereto, and enhance the prestige of the Profession.
5) My country, therefore, in my personal, business and social contacts, I shall at all times uphold my nation, respect and honour the chosen way of life of fellow citizens, be law abiding, transparently honest, of unquestionable integrity, and utmost responsibility and reliability.

Each entity of the code of conduct has a direct bearing on how members of the profession are expected to relate in the society: with clients, employers, professional colleagues.
All members of the profession are expected to understand the roles laws and ethics has for them to carry out their duties. There are penalties and punishments of varying degrees for different cases of misconduct or misdemeanor.

3. CYBER-SECURITY AND CYBERCRIME

The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. The term "cybercrime" is used to cover a wide variety of criminal conduct.
Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime describes a range of circumstances in which technology is involved in the commission of crime. It presents numerous and constantly evolving challenges to government and law enforcement (Jonathan, 2011). Kumar in 2003 defined Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

3.1 Cybercrime and Cybercriminal Offences and Categories

Csonka (2000) in his paper entitled Internet Crime maintained that the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders as of 2000 categorized five offenses as cyber-crime:

1. Unauthorized access
2. Damage to computer data or programs
3. Sabotage to hinder the functioning of a computer system or network
4. Unauthorized interception of data to, from and within a system or network
5. And computer espionage.

Abasiama (2019) categorized cyber criminals that is individuals who perpetuate cybercrime into 4 different categories:

1. black hats: individuals with extraordinary computing skills, who resort to malevolent or destructive activities, with a view to bringing down an existing system they are also called crackers.
2. white hats: individuals who possess hacker skills but use them for defensive purposes. They are called security analysts or ethical hackers.
3. gray hats: individuals who work both offensively or defensively depending on the immediate circumstances and prevailing situations.
4. suicide hackers: individuals who aim to bring down critical infrastructure for a personally identified "cause" without minding the dire consequences of such an act, even including going to jail for a long period of time.

Typical examples of computer crimes include but are not limited to embezzlement, fraud, financial scams and hacking (Ajayi, 2016). Mohammed et al (2019) state that cybercrime is an umbrella term used to describe two distinct but closely related criminal activities: cyber-dependent and cyber-enabled crimes. The former are offences that can only be committed by using a computer, computer networks, or another form of ICT. These acts include the spreading of viruses and other malicious software, and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another form of ICT. This includes but is not limited to fraud (including mass-marketing frauds, phishing e-mails and other scams; online banking and e-commerce frauds); theft (including theft of personal information and identification-related data); and sexual offending against children (including grooming, and the possession, creation and / or distribution of sexual imagery) (McGuire & Dowling, 2013).

Sager (2000) stated that cybercrime and cyber-security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cybersecurity addresses cybercrime as one major challenge underscores this. Cybersecurity plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.

3.3 Extant Laws to Combat Cybercrime in Nigeria

There are four laws recognized in Nigeria to combat cybercrime:

1. The Nigeria Criminal Code Act 1990
2. The Economic and Financial Crime Commission Act, 2004 (Source: National Assembly of Nigeria, 2004)
3. Advance Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria, 2006)
4. Cybercrimes (Prohibition, Prevention, etc) Act, 2015

The Nigerian Cybercrime Act (2015) provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This Act also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furtherance of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

The Nigerian Cybercrime Act 2015 prescribes the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual (amongst other punishments for lesser crimes).Under the Cybercrime Act 2015 in Nigeria, hackers, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

The Cybercrime Act 2015 makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment. Okonigene and Adekanle (2010) inform that an example of identity fraud would be the individual who impersonated Chief Bola Tinubu (a Nigerian politician) on Facebook and was apprehended by the police.

- It specifically creates child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.

- Outlaws Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.
- Prohibits cybersquatting, which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.
- Forbids the distribution of racist and xenophobic material to the public through a computer system or network as well as on social media platforms (e.g. Facebook, Instagram, emails, Whatsapp and Twitter), it also prohibits the use of threats of violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less thanN10million or to both fine and imprisonment.
- The Cybercrime Act 2015 mandates that service providers shall keep all traffic data and subscriber information having due regard for the individual's constitutional right to privacy, and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.
- Allows for the interception of electronic communication, by way of a court order by a judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

The Act itself contains 43 sections, and is a very important piece of legislation to foster the development of the nascent ICT sector in Nigeria.

4. RECOMMENDATIONS AND CONCLUSION

Law and ethics are different in a manner that what a person must do and what a person should do. The former is universally accepted while the latter is ideal human conduct, agreed upon by most of the people. However, both the law and ethics are made in alignment so that they do not contradict each other.

In light of present contemporary happenings, there is the need for all and sundry to recognise that laws and policies evolve at a much slower rate than technology. It is imperative for all (and not only IT Professionals) to handle our use of technology with caution. Our ethical, moral and indeed religious convictions should allow us to give much care and deep thought to our handling of technology (and social media) so as not to run foul of the law or perform actions that could be potentially injurious to others.

Also, the Information Technology profession like all other professions has an explicitly spelt out code of conduct and ethics that is expected to be binding on their members. While professional organizations can prescribe ethical conduct, they do not always have the authority or legal backing to banish or deter violators from carrying out their activities. The Computer Professionals Registration Council of Nigeria should be encouraged to ensure that its members obey the clearly spelt out laws of the land and by follow to the letter the codes of conduct of their profession. Deterrents can be put in place for members who have earned some level of certification or professional accreditation. Professional bodies are called upon to use their "muscle" and their "teeth" to enforce the punitive aspects of their professional code of conduct. These could include the threat of loss of accreditation or certification due to a violation of a code of conduct, bearing in mind that loss of certification or accreditation can dramatically reduce members' marketability and earning power.

It is the responsibility of IT professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. If this is done no IT practitioner will be an accomplice in carrying out cybercrime. Cybercrime is a threat to the economy of a nation as well as its peace and security. Ensuring that IT practitioners are well aware of what is expected of them will go a long way in curbing this menace.

REFERENCES

1. Abasiama, G. A.(2019). Cybercrime and Cyber security: A Painted Scenario of a New Type of War. CSC Lecture Series 19. Evangel University, Akaeze – Nigeria.
2. Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12.
3. Csonka P. (2000). Internet Crime; the Draft council of Europe Convention on Cybercrime: A response to the challenge of crime in the age of the internet? Computer Law & Security Report. 16(5).
4. Foote D. (2002). Good Ethics at Work Lie in the Hiring. Computerworld. Retrieved July 3, 2019 from http://www.computerworld com/printthis/2002/0, 4814,68719,00.html
5. Jonathan, C. (2011). Cybercrime. Commonwealth Law Bulletin, 37(4), 671-680
6. Khalid A. (2004). Cybercrime: Business and the law on different pages. The Star. Retrieved July 3, 2019 from http://www.niser.org.my/news/2004_03_05_01.html
7. Kumar, K. (2003). Cyber Laws, International Property and e-commerce Security, Dominant Publishers and Distributors New Delhi.
8. McGuire, M., & Dowling., S. (2013). Cyber-crime: A review of the evidence summary of key findings and implications. Home Office Research Report 75, Home Office, United Kingdom, October. 30p.
9. McQuade, S. 2006. Understanding and Managing Cybercrime, Boston: Allyn & Bacon.
10. Mohammed, K, Mohammed, Y, & Solanke, A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. International Journal of Cybersecurity Intelligence and Cybercrime, 2 (1), 56-63.
11. Okonigene, R.E. and Adekanle, B. (2010). Cybercrime in Nigeria. Business Intelligence Journal. 3(1) 98
12. Sager, I. (2000). Cyber Crime. Businessweek Online. Retrieved July 3, 2019 from http://www.businessweek. com/2000/00_ 08/b3669001.htm
13. Telephone Consumer Protection Act of 1991 Section 40 of Economic and Financial Crimes Commission (Establishment) Act 2004.
14. http://lawnigeria.com/LawsoftheFederation/Cyber-Crime-Act,-2015.html
15. www.itu.int/dms_pub/itut/oth/0A/0D/T0A0D00000A0002MSWE.doc.
16. www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-workprogramme-developing-countries.pdf.
17. www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf