AN OVERVIEW OF SOCIAL MEDIA RELATED CYBERCRIMES AND ITS LEGAL REMEDY*

Abstract

The internet with its open system design and emphasis on ease of communication, presents a particularly difficult balancing between criminal actions and authorized use. The emergence of various social media platforms has created an enabling environment for an increase in cybercrimes. This work was motivated by the fact that what constitutes cybercrime is inexact because of a lack of consensus of what should be included in the measurement. This paper presents the various ways cybercrimes are carried out on different social media platforms. This poses a challenge as there are no identification verification processes. The purpose of this paper is geared towards determining to what extent the exponential growth in social media usage has facilitated cybercrime. In this paper, we adopted the doctrinal method of legal research. The paper finds that anonymity, low cost and ease of operation on social media platforms has made it increasingly an attractive place to do business. The paper finds that the threat of cybercrime can be greatly minimized by creating awareness of such crimes. The paper concludes by stating that there is need for the development of a cybercrime related legal framework for checkmating social media cybercrimes. It recommends among many, that sharing of personal information/data should be avoided on social media platforms.

Keywords: Social media, cybercrime, internet crime, cyber security, legal remedy

1. Introduction

Millions of communications take place daily on social media platforms. Social media has effectively built a vast and formidable platform, not just for sharing ideas and pictures, but also as a playground for cybercrime.[1] Social media is also a deep pool of personal data. People feel safe to share personal details on social media platforms. However, without due care, personal data, such as name, phone number, address and even one's location can be stolen and used for identity theft or the creation of synthetic identities. However, it is pertinent to note that social media is not all bad. It offers a way to keep in touch with family and friends. It also offers platform for sales, advertising and wider audience reach within splits of seconds. Professional versions of social media, such as LinkedIn, are an important way to keep up with industry intelligence. Presently, social media platforms are fast becoming part of human being's daily lifestyle, where millions of persons are users of internet-based social media platforms. Despite its several benefits, social media has posed a huge risk that leads to adverse impacts. Cyber criminals have turned to social media as an outlet for carrying out their criminal actions.[2]In a world where people easily provide their private details because they are attracted by these social media platforms. Cyber criminals utilize them as a lure to get the information they require. Computers and the internet are used in carrying out cybercrimes by stealing other people's identities as well as tracking down personal information and victims. Regrettably, social media has been preferred outlet for cybercriminals to carry out their nefarious acts.[3] It is therefore unsurprising that the emergency of social media has brought in its wake multiple vectors of criminal behaviour. What is just needed to commit crime is a computer or phone, access to the internet and criminal intent.[4] Social media provides anybody the power to circulate commercially delicate details as well as spread untrue details, which could be damaging. Hence, there is need for content monitoring and control by the providers of social media platforms.

2. What is Cybercrime?

Cybercrime also called computer crime, is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating privacy.[5] It is also defined as an 'umbrella' term for lots of different types of crime which either take place online or where technology is a means and/or target for the attack.[6] A cyber dependent crime is an offence that can only be committed using a computer, computer networks or other form of information

***By N.O. UMEJIAKU, PhD, BL,** Senior Lecturer and Head, Department of Commercial and property Law, Faculty of Law, Nnamdi Azikiwe University, Awka. Phone no: 08033809219; and

***N. C. UZOKA, PhD,** Lecturer, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka. Phone no: 08063212174. Email: chisongozi@yahoo.com

[1] How Social Media is used in Cybercrimes. Available at http://www.thedefenceworks.come Accessed on May 14, 2021.

[2] L Almadhoor, Social Media and Cybercrimes, (2021) *Turkish Journal of Computer and Mathematics Education,* 3.

[3]N Al Mutawa, I Baggali & A Marrington, 'Forensic Analyzers of Social Networking Applications or Mobile Devices' (2012) Digital Investigation,

[4]Myar, 'A Failure to Regulate? 'The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media' (2018) *International Journal of Cyber Security Intelligence and Cybercrime.*

[5] What is Cybercrime? Available at https://www.britannica.com Accessed on 20th June, 2021.

[6] What is Cybercrime? Available at https://www.bedfordshire.police.uk Accessed on 20th June, 2021.

communications technology.[7] Cyber enabled offences are referred to those offences that are facilitated by our ever-growing technological capacities for example online fraud, online trade in illicit goods such as drugs or firearms and online child sexual-exploitation and abuse.[8] Cybercrime is also related to people's privacy.[9] The Council of Europe's Cybercrime Treaty uses the term 'cybercrime' to refer to offences ranging from criminal activity against data to contact and copyright infringement.[10]

However, Zeriar-Geese,[11] suggests that the definition is broader, including activities such as fraud, unauthorized access, child pornography and cyber-stalking. The United Nations Manual on the Prevention and Control of Computer Related Crimes includes fraud, forgery and unauthorized access in its cybercrime definition.[12] It is pertinent therefore to state that there is no catchall term for the tools and software which are used in the commission of certain online crimes. Despite an apparent acceptance of and familiarity with the term, there exist dramatically different views of what cybercrime is. This lack of generally accepted definition is problematic as it affects every aspect prevention and remediation.[13]

3. Types of Social Media Cybercrimes

Hacking: This is a term used to refer to an act committed by an intruder by accessing your computer system without your permission.[14] It also means illegal access to any digital devices or a computer done through various social media forums.[15] Hackers (the people doing the act of hacking) are basically computer programmers who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. Hackers break into systems to steal personal banking information, a corporation's financial data etc. They also try to modify systems so they can execute tasks at their whims and caprices. Hackers also distribute messages to individuals via social media. This occurs when the user clicks on those individual links and consequently gets attached by criminals. Hackers make extensive use of online communities, sharing knowledge, tools, as well as performing coordination and recruitment activities.

Cyber Stalking: This is often done through horning or intruding into the individuals' private life to trigger distress, stress, worry and anxiety.[16] Cyber stalking involves the act to pursue, harass or contact another in an unsolicited manner using electronic medium.[17] Cyber stalking bothers a person psychologically as a result it is actually regarded as 'psychological statutory offense' or even 'mental offence'. A cyber stalker can terrorise his or her victim as anonymity leaves the cyber stalker in an advantageous position. This anonymity can be achieved by using a number of methods like using obsolete versions of computer software called 'mail daemons'' or entirely false users details during online registration on social media platforms.[18] A cyber stalker may also use email threats that contain offensive materials such as nude photographs, videos showing abuse or obscenity and posting nasty comments that may be used and may cause the victim to feel annoyed, violated and emotionally anxious.[19]

Phishing: This is a technique of extracting confidential information such as credit card numbers and username, password combination by masquerading as a legitimate enterprise.[20] Phishing is typically carried out by email spoofing. In phishing, the attackers use names and logos of well-known websites to deceive their victims. The graphics and the web addresses used in the email are strikingly similar to the legitimate

[7]M McGuide & S Dowling, 'Cyber Crime: A Review of the Evident Summary of Key Findings and Implications. (2013)Home Office Research Report, 75.
[8] Cybercrime – United Nations Office on Drugs and Crime, Available at https://www.unodc.org Accessed on 21, June, 2021.
[9] *Ibid*
[10] T Krone, 'High Tech Crime Brief', Australian Institute of Criminology (2005)
[11]Z Geese, The State of the Law on Cyber-jurisdiction and Cyber-Crime on the Internet, California Pacific School of Law, (1998) *Gonzaga Journal of International Law*, 18.
[12]The United Nations Manual on the Prevention and Control of Computer Related Crime, (1995) International *Review of Criminal Policy* 44.
[13] S Gordon and R Ford, 'On the Definition and Classification of Cybercrime,' (2006) *13Journal in Computer Virology.*
[14] The 12 Types of Cyber Crime. Available at https://www.digi.in/technology/guides Accessed on 14th May, 2021
[15]Alferidah, D Khalid and N Z Ihanjhi, 'A Review on Security and privacy Issues and Challenges in Internet of Things' *International Journal of Computer Science and Network Security* (2020) Vol. 20 No. 4
[16] *Ibid*
[17]G Sunil, S Aluvala *et al*, Various Forms of Cybercrime and Role of Social Media in Cyber Security', (2020) *International Journal of Advanced Science and Technology* ,Vol. 29 No. 2.
[18] *Ibid*
[19]H Mal-Khateeb and G Epiphaniou, 'How Technology can Mitigate and Contract Cyber-Stalking and Online Grooming', (2016) *Computer Fraud and Security Journal* 1
[20] The 12 Types of Cyber Crime, *op cit*

ones, but they are designed to lead you to funny sites. However, not all phishing are done via email or websites. Voice phishing (vislung) involves calls to victims using fake identity fooling one into considering the call to be from a trusted organization.[21]

Malware: Malware is malicious software designed to cripple or take over your computer system.[22] It damages devices, steals data and causes chaos. Malware is a contraction of malicious software created by a team of hackers to carry out nefarious activities. Malware is the force behind most cyber attackers. It installs a virus in the users system when the user clicks on links it doesn't recognise or open attachments sent by people in your friend list, the user is opening itself up to a potential malware infection. It is important that users of social media should always verify that the source of a file is legitimate before clicking on or downloading any files. Types of malware include, virus, Trojans, worms, transom ware, adware and botnets. For example, Trojan is a worm containing secret code for stealing an individual's confidential information.[23]

Identity Theft: Identification fraud is a form of fraud in which a person claims to be someone else as well as performs criminal activity online with the title of another person.[24] It is one of the commonest social media cybercrime. A person can steal another person's relevant information like name, address, pictures to pose as an individual to commit crime like defrauding unsuspecting members of the public. The wrong doer can even use the fake account or profile to transact with companies and organizations.

Theft of FTP Passwords: This is another very common way to tamper with one's information on their websites or phone.[25] The FTP password hacking takes advantage of the fact that many people/webmasters store their website login information on their poorly protected phones and computers. The criminal searches the victims system for FTP login details and then relays them to his own remote computer.[26] He then logs into the web site/platform via the remote computer and modifies the web pages/platform as he or she pleases. With this, the criminal will have access to the victim's bank accounts and other mobile based application websites.

Credit Card Fraud: Credit card or debit card fraud is a type of identity theft in which an unauthorized person uses someone's credit card information for withdrawing cash from it or makes purchases.[27] Criminals use the internet for credit card fraud or do it in person. This unauthorized use can be done in various ways, using lost or stolen card, account takeover by reporting card lost or stolen after getting sufficient information and by skimming, which involves an electronic attachment that appears valid such as a self service credit card swipe at a gas pump etc.[28]

The above social media related crimes are the most common types. Hence, there are many crimes being committed on the social media space/platforms.

4. Current Legislation Regulating Cybercrimes in Nigeria

The aim of this section is to discuss the legal framework on cybercrime in Nigeria.

Cybercrimes (Prohibition, Prevention, etc) Act 2015[29]

This is the principal legislation for acts of cybercrime in Nigeria. The Act provides a comprehensive regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act made elaborate provisions on identity theft and impersonation[30], child pornography and related offenses[31], cyber stalking[32], cyber squatting[33], phishing, spamming, and spreading of computer virus. The office of the National Security Adviser is the coordinating

[21] *Ibid*
[22] What is Malware, available at https://www.avg.com. Accessed on 20th July, 2021.
[23]M. R. Faghami, A Matrawy and C H Lung, 'A Study of Trojan Propagation in Online Social Networks,' in 5th International Conference on New Technologies, Mobility and Security (2012).
[24] G Sunil, A Alurala *et al, op cit*
[25] The 12 Types of Cybercrime, *op cit*
[26] *Ibid*
[27]T R Soomro and M Hussain, 'Social Medra-Related Cybercrime and Techniques for their Prevention' available at https://www.researchgate.net. Accessed on 10th May, 2021.
[28]*Ibid*
[29] Cybercrime (Prohibition, Prevention, Etc,) Act 2015. Available at https://www.cert.gov.ng Accessed on 21st June, 2021.
[30] Section 22 Cybercrimes (Prohibition, Prevention, etc) Act 2015.
[31] Section 23 , *Ibid*
[32] Section 24 , *Ibid*
[33]Section 25, *Ibid*

body for all security and enforcement agencies under the Act.[34] A Cybercrime Advisory Council was also established by the Act to among other duties formulate and provide general policy guidelines for the implementation of the provisions of the Act. The Federal High Court vested with jurisdiction to try offences under this Act.[35] It is pertinent to note that offence under this Act shall be extraditable under the Extradition Act, CAP E25 LFN, 2004.[36] The Act provided for unauthorized access to a computer for fraudulent purpose and for obtaining data vital to national security as an offence punishable with a term of five years[37] imprisonment or a fine of not more than ₦5,000,000.00 (five million naira) or to both fine and imprisonment.[38]Where such offence is committed with the intent of security access to classified information relating to commercial or industrial secret, the offence is punishable with imprisonment for a term of not more than seven years or a fine of not more than five million naira or 7 years imprisonment or to both fine and imprisonment.[39] The Act in this section raises the issue of 'intent' to commit a crime. Intention to commit a crime is difficult to prove.[40] The law enforcement agencies may not have the wherewithal to categorically pin the accused to the crime as it may be difficult to prove intention in cyber activities where clicking a button may lead to various results.[41]

Criminal Code Act[42]

The Criminal Code Act is among the foremost Act regulating crimes in Nigeria. It provides that any person who by an false pretence, and with the intent to defraud, obtains from any other person anything capable of being stolen or induces any other person to deliver anything capable of being stolen is guilty of a felony and is liable to imprisonment for three years[43]. The Act also provides that, any person who by means of any fraudulent trick or device, obtains from anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen or to pay or deliver to any person any money or goods, or any greater sum of money or greater quantity of goods than he paid for or would have been delivered but for such trick or device is guilty of misdemeanour and is liable to imprisonment for two years.[44] These provisions as laudable it may seem are old fashioned and predates the internet regime. It did not address internet and cyber crimes specifically. The archaic nature is made manifest in Section 419 which provides that unless the criminal is caught in the act, such criminal cannot be arrested without warrant. Cyber criminals are very smart and only in exceptional cases that a cyber criminal can be caught in the very act.

Penal Code Law [45]

This Law applies only to the Northern Part of Nigeria. It contains some provisions that may be used in prosecuting cybercriminals in the area of counterfeiting and forgery. Section 320 provides that whosoever by deceiving a person; (i) fraudulently or dishonestly induces the person so deceived to deliver any property to a person or consent that any person shall retain any property or (ii) intentionally includes the person deceived to do or omit to do anything which he would not do or omit to do if he were not so deceived and which act or omission cause or is likely to cause damage to that person in body, mind reputation or property is said to cheat[46]. Section 362 also provides that, a person who dishonestly makes, signs, seals or executes a document or part of it with the intent of making others to believe that the document is made by the authority authorised to so make, without lawful authority, alters a document or part of it with the intent of deceiving others to believe that the document emanates from a lawful authority commits forgery. The above two provisions of the Penal Code may be employed in tackling phishing, forgery and counterfeiting. However, this is also an old law that will not deal extensively with cybercrimes particularly on social media platforms.

Money Laundry (Prohibition) Act 2011[47]

This Act prohibits the laundry of proceeds of crime or an illegal act. It provides that no person or body corporate shall except in a transaction through a financial institution, make or receive cash payment of a sum

[34] Section 32 , *Ibid*
[35] Section 41, *Ibid*
[36] Section 50, *Ibid*
[37] Section 51, *Ibid*
[38] Section 6(1) *Ibid*
[39] Section 6(2) *Ibid*
[40]U V Awhefeada & O O Bernice, Appraising the Laws Governing the Control of Cybercrime in Nigeria, (2021) *Journal of Law and Criminal Justice* Vol. 8 No. 1.
[41] *Ibid*
[42] Cap C 38, Laws of the Federation 2004.
[43] Section 419 Criminal Code Act 2004.
[44] Section 421 Criminal Code Act, 2004.
[45] Cap P3, Laws of the Federation 2004.
[46] See Section 320 (1) & (b) Penal Code Act.
[47] Cap M18, Laws of the Federation, 2004.

exceeding N5,000,000.00 (5 million) or its equivalent in the case of an individual or N10,000,000.00 (10 million) or its equivalent in case of a body corporate.[48] From the foregoing provision, transactions exceeding the stated amount are to be reported to the Central Bank of Nigeria, Securities and Exchange Commission or the Economic and Financial Crime Commission. This Act made extensive provision for cyber security and measures to guard against cybercrimes only in the financial institutions. It failed to address other types of cybercrimes.

Economic and Financial Crime Commission Act 2004[49]

The Act made extensive provisions with respect to financial crimes. The Commission is charged with the responsibility of the following:

i) The investigation of all financial crimes, including advanced fee fraud, money laundry, counter-feiting, illegal charge, transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam among others.
ii) The coordination and enforcement of all laws against economic and financial crimes with a view to identifying individual, corporate bodies or groups involved.
iii) The coordination of all investigating units for existing economic and financial crimes in Nigeria.[50]

The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1994, the Failed Bank (Recovery of Debts) and Financial Malpractices in Banks Act 1994 (As Amended) and the Banks and other Financial Institution Act 1991 (As Amended) and Miscellaneous Offences Act.

5. Cyber Security Laws in Some Other Jurisdictions

Australia: Australia's Parliament passed a controversial law designed to prevent the 'weaponisation' of social media platforms. The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, which amended the Criminal Code Act of 1995 by introducing offences for failing to notify of abhorrent content, and failing to take down abhorrent content.[51] The Act requires that internet service providers, content service providers and hosting service providers are to notify the Australian Federal Police within a 'reasonable time' if any abhorrent violent material involving abhorrent conduct in Australia is available on the service providers' platform, whether or not the provider is in Australia. That is, this applies to all platform providers around the world, if they host or make available the relevant material. Failure to notify and failure to remove the relevant content attracts heavy penalties.[52] Cyber crime, albeit, abhorrent violent material is placed on the internet service providers to decipher. This means that the different social media platforms are to be held responsible for any crime emanating from their platform. Abhorrent violent conduct was defined as conduct whereby a person engages in a terrorist act, murders another person, attempt to kidnap another person.[53] It is submitted that the scope of this Act is limited in application, as it did not cover other forms of social media cybercrimes. However, this move by Australia has made social media platforms like Facebook to employ a huge number of content checkers and increasingly engage with third party content verifiers. There is also established in Australia eSafety Commissioner under the Enhancing Online Safety Act of 2015, to promote online safety for all Australians.[54] The eSafety Commissioner administer the Online Content Scheme, which provides a complaints mechanism for prohibited content based on the classification categories in the National Classification Scheme.. However, there have been calls for the review and upgrade of this law to Online Safety Act and a new single code of industry practice.

China: In China, sites such as Twitter, Google and WhatsApp are blocked.[55] Their services are provided instead by Chinese Providers such as Weibo, Baidu and WeChat. Chinese authorities have also had some success in restricting access to the viral private networks that some users have employed to bypass the blocks on sites. The Cyberspace Administration of China announced at the end of January, 2019, that in the previous

[48] Section 1 of Money Laundering Act 2011.
[49] Cap E10, Laws of the Federation of Nigeria, 2010.
[50] Part 2 of the EFCC Act 2004.
[51] Social Media Execs will Face Jail in Australia If their Platforms Host Violent Content. Available at https://www.cnbc.com Accessed on 20th June, 2021.
[52] *Ibid*
[53] *Ibid*
[54] M Biddington, 'Regulation of Australian Online Content: Cybersafety and Harm', Available at https:www.aph.gov.au,accessed on 20th July, 2021.
[55] Social Media: How do other Governments Regulate it? Available at https://www.bbc.com, accessed on 24th June 2021.

six months it had closed 733 websites and 'cleaned up' 9,382 mobile apps being used for illegal purposes thank social media.[56] China has hundreds of thousands of cyber police, who monitor social media platforms and screen messages that are deemed to be politically sensitive. China also invested on Security technology, imposing requirements on the e-commercial enterprise and surveillance on users. Specific regulation on cybercrime started in 1994 when the state promulgated the ordinance on Security Protection of Computer Information System (State Council Decree No. 147, 1994).[57] The Ordinance prescribed legal liability for five types of activities: (a) violating security ranking protection systems of computer information systems and threatening the computer information systems; (b) violating the registration system of computer information systems international networking (c) not reporting cases that happened in the computer information systems according to the prescribed time (d) refusing to improve after receiving the notice from the public security agency requiring improving the security situation and (e) other acts threatening the computer information system[58]. The main problem with China's substantive law provisions is that there was overlap of provisions, missing of referred regulations and laws and laggard penalties. However, China took a series of actions characterized by content filtering and activity monitoring, for the purpose of maintaining state stability as well as cyber security.

United States of America: The Federal Government is yet to pass laws that give a comprehensive treatment of cyber security. However, there are some pieces of legislation aimed at checkmating cybercrimes. They include; Children's Online Privacy Protection Act of 1998, the Sarbanes Oxley Act of 2002, Federal Information Security Management Act of 2002, Federal Information Security Modernization Act 2014, and Cyber Security Information Sharing Act 2015. In addition to the federal laws and regulations, a number of states have passed their own more comprehensive cyber security laws. Instances are California Consumer Privacy Act 2018, New York Stop Hacks and Improve Electronic Data Security Act 2019. In addition to the various state laws across the United States, global companies are expected to adjust their cyber security measures to comply with international laws.

6. Conclusion and Recommendations

The fast development and wildfire usage of social media networking platforms has, as with other internet-related practices, brought to the fore front a wide range of social media cybercrime problems that have an increasingly negative impact. It is pertinent to note that the foremost way of controlling social media crimes is through the media companies by way of self-regulation and voluntary content control. This will be supported by the government and third party actors who offer additional support through policy framing, voluntary initiatives and educational sensitization. There are a number of issues that have prevented the accurate measurement and tracking of cybercrime. Firstly, the lack of a clear definition of what constitutes cybercrime. This is compounded by the facts that the range of cybercrimes is ever expanding in the globalized world and cybercrimes often overlap with non-cyber crimes, thus providing challenges in gauging the true scope of cybercrimes. The following measures may be helpful. These should be enacted in Nigeria an all encompassing law which will cover all forms and types of cybercrime. There should be established a cyber-tribunal for speedy and effective disposal of cybercrime related cases. There is need to amend both the Criminal Code and the Penal Code to be in line with the modern day technological innovations and realities. The different states of the Federation should also create their own laws on cyber security as is obtainable in the United States of America. Cyber police/monitors should be formed to prevent, deter and detect cyber crimes. The Nigeria government should invest heavily on security technology, as well as impose requirements on electronic commercial enterprises and surveillance on users. The general public should be sensitized on the workings and *modus operandi* of cyber criminals. The providers of social media platforms and networking sites also need to be on the alert as to the contents shared on their platforms so as to forestall cybercrimes.

[56]L Xingan, 'Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crimes', (2019) *International Journal of Cyber Criminology*.
[57] *Ibid*
[58] L Xingn, *op cit* .