journals.unizik.edu.ng/jcpl/index ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW Vol. 12(5), October, 2025

CYBERSECURITY LAWS AND PRIVACY PROTECTION IN NIGERIA: A REVIEW

Kelvin BRIBENA*

Abstract
The study looked at cybersecurity risks and cybercrime, with a focus on Nigerian laws intended to protect people' digital assets and privacy as well as the integrity of state institutions. It used a doctrinal research methodology, examining Nigeria's current cybersecurity legislation. This approach provided a practical way to deal with a complicated problem that was changing quickly. The study heavily relied on online materials, including government studies and corporate sector publications that offered insight into worldwide practices, and explored a wide range of digital resources. The study used declassified and publicly accessible materials, including official websites and legal platforms, to examine Nigerian laws and regulations pertaining to cybersecurity and cybercrime. These sources provided clarification on the purpose and operation of these laws. It evaluated their efficacy and emphasised the need for further legislative and regulatory initiatives to improve protection for people, organisations, society, and the economy in the digital age. Although the scope of this right varies by nation from limited acknowledgement in some states to constitutionally established safeguards in others, the study recognised that privacy is a basic value that extends beyond people to organisations and institutions. It noted that data abuse has grown widespread, especially through illegal activity. The research also identified flaws in Nigeria's cybersecurity architecture, pointing out that although there are regulations, they are frequently not adequately enforced or prosecuted. According to the argument, Nigeria has not yet acknowledged cybersecurity as a crucial element of national security. In the conclusion, the research stressed that the benefits of adopting digital technology much exceed the drawbacks and advised the active participation of all stakeholders. Adoption of digital technology improves everyday life, boosts the economy, creates jobs, and has major societal advantages including better educational and healthcare outcomes.

Keywords: Nigerian Legal System, Cybersecurity, Law Enforcement

1. Introduction

Wikipedia notes that more than 150 national constitutions explicitly recognize the right to privacy, underscoring its status as a globally acknowledged fundamental human right. This demonstrates the widespread concern for privacy protections. However, balancing the benefits of cyberspace with safeguarding citizens' privacy often involves trade-offs.[1] Cybersecurity laws are therefore essential, as they aim to curb cybercrimes that threaten the privacy and digital assets of individuals and institutions.[2]

Cybercrime is a universal challenge, carried out electronically and with significant implications for the economic stability and security of nations. With the rapid worldwide expansion of electronic platforms and communication technologies—many of which are replacing older, less secure systems—there has been a dramatic rise in both the number and variety of cybercrimes. This reality highlights the urgency for governments to invest heavily in cybersecurity infrastructure and to enact effective laws that defend privacy, digital property, and related assets.

Scholars and experts have pointed out critical issues in this field. Chief among them is the unprecedented pace of technological change. While digital innovations contribute immensely to

***Kelvin BRIBENA** PhD, Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria. Email: kelvinbribena@gmail.com

[1] 'Read about "Right to privacy" on Constitute' constituteproject.org. Retrieved 10 May 2024

[2] citation: Various internet sources

global economic development, abuses in cyberspace are expanding more quickly than security mechanisms can respond. Although private sector solutions exist, they often come at a cost that makes them inaccessible to many users.

In examining Nigeria's institutions and policies on cybercrime, important questions arise: What position does Nigeria occupy in terms of adopting a national framework for data privacy? And what initiatives could strengthen the nation's ability to confront privacy threats while advancing equitable cybersecurity laws and enforcement? These questions are crucial because cyber technologies are now deeply woven into political, economic, and social systems, shaping modern society on a global scale. The cyber realm-dominated by computers, networks, and diverse digital devices-has grown into a multi-trillion-dollar industry with enormous influence on global affairs.

Cybersecurity legislation seeks to secure personal and institutional data against unauthorized access and misuse. Such laws cut across nearly every aspect of contemporary life, from protecting sensitive records in hospitals, schools, banks, and businesses, to safeguarding government databases and the personal information of households and individuals.

There are several classifications for cybercrime perpetrators. Among them are:
State-sponsored actors Russia, Iran, North Korea, and China are frequently mentioned in literature as examples of governments that have been connected to cybercrimes. Nonetheless, the majority of countries probably participate in cyber operations to some extent. The suspected Russian meddling in the 2016 U.S. presidential election is a well-known example.

Entrepreneurial cybercriminals might be reputable organisations like banks that profit from illicit money laundering, private citizens like hackers or ransomware attackers, or organised crime organisations like terrorist networks, mafias, and gangs.

The purpose of cybersecurity is to prevent illegal activity in cyberspace.[3]Globally, internet usage has increased quickly, and younger generations are adopting it at an accelerated rate. But this growth has also made people more vulnerable to other online dangers. Because of this, putting robust cybersecurity safeguards in place has become essential. Over $500 billion is lost to the global economy each year as a result of cybercrime, which also threatens people's livelihoods through data theft and abuse and results in job losses in the US. Business Email Compromise (BEC) is a particularly harmful type of cybercrime in which hackers get access to corporate email accounts and pose as their owners in order to trick partners, clients, or workers into sending money or private information. For example, Ramon Olorunwa Abbas, also known as Hushpuppi, is a Nigerian scammer who is being prosecuted for using BEC techniques to illegally collect over $922,000.[4]

According to reports from the Nigerian Communications Commission (NCC), the economic cost of cybercrime has increased globally rather than decreased. These days, hackers employ sophisticated toolkits, browsers, and plugins to make assaults easier. Due in large part to lesser chances of being caught, many of these crimes are committed from poor countries like Nigeria, Ghana, and India and target developed nations like the United States and the United Kingdom.[5] Nigeria has also suffered severe economic losses as a result of cyberterrorism, with an estimated ₦127 billion in lost GDP. It has a noticeable effect on financial markets, banking, foreign investment, and citizens' trust in internet transactions[6].

[3] Nigeria Communications Commission - Department of New Media and Information Technology
[4] https://www.bloomberg.com/features/2021-hushpuppi-gucci-influencer/
[5] ibid
[6] ibid

2. Conceptual Clarification

A. Protection of Cyberspace

The procedures intended to protect cyberspace against dangers from extremists, cyberterrorism, and unauthorised access are referred to as cybersecurity. It developed in reaction to the rise in numerous types of cybercrimes. Strong cybersecurity regulations protect private information and stop bad actors from using it against you. A common topic of discussion is how to strike a balance between privacy and security. The confidence of the populace declines when national systems are not trusted. However, no country can completely ensure privacy, particularly in light of the rising threats of terrorism and cyberwarfare. Despite being a basic right, privacy is still not sufficiently protected under Nigeria's cybersecurity framework.

B. Personal Space

Many legal systems uphold the right to privacy, protecting people from excessive interference by public or private organisations. This freedom is recognised by more than 150 national constitutions, including the 1999 Constitution of Nigeria (as modified). In a similar vein, Article 12 of the 1948 Universal Declaration of Human Rights states that everyone has the right to legal protection from arbitrary intervention in their personal lives, families, or correspondence[7].

The viability of protecting privacy in the current digital era is still up for dispute, though, particularly in light of governments like the Australian and British ones defending more monitoring in the name of national security. Although it may seem that monitoring violates people's rights, it is frequently justified as being required to stop terrorism and crimes. Despite criticism, Russia has implemented strict internet legislation to defend sovereignty and, in contrast to many Western countries, places a higher priority on national security than privacy. However, there are still significant loopholes in Nigeria's cybersecurity, leaving its residents at risk of privacy abuses, particularly in the face of online terrorism and extremist activities.

The following are important points in the privacy-security debate:
Sometimes privacy must be sacrificed for security.
Cybersecurity is essential to privacy because it protects personal information.
In the end, privacy and cybersecurity are not mutually exclusive; nonetheless, security should come first when there are serious national security risks.

C. Online fraud

Although the internet has made the globe a smaller place, it has also contributed to the growth of cybercrime. Many Nigerians, particularly young individuals, have been lured into internet fraud by lax enforcement, unemployment, greed, and a lack of education. These activities have extended beyond Nigeria to other West African nations under ECOWAS free-movement rules.

Among those committing cybercrime are:
Youth who are very proficient in digital technologies but have no desire to pursue further education or employment in the workforce[8].
Bank insiders who take use of institutional system expertise[9].
Fraud-facilitating individuals with international ties.
Dishonest security personnel who aid criminals[10].
There are several types of cybercrimes:
Cyberterrorism: Using extortion or hacking to target governments or organisations in order to get information or further political goals.

[7]https://en.wikipedia.org/wiki/Right_to_privacy
[8]Journal of Law, Policy and Globalization www.iiste.org ISSN 2224-3240 (Paper) ISSN 2224-3259
[9]The International Journal of Engineering and Science (IJES)| |Volumel12 ||Issue||4
[10] ibid

Cyberstalking is the practice of persistently harassing someone online by threatening, bullying, or intimidating them.
Malware: Trojan horses or viruses intended to harm or access systems without authorisation.
Fraud and identity theft, commonly referred to as "Yahoo Yahoo," are prevalent in Nigeria and include deceit in order to steal money or information.
Drug trafficking: New ways to sell illegal drugs have been made possible via the internet, sometimes through covert online networks.

3. Nigeria's Prominent Cybercrime Laws

Prior to the 2015 Cybercrime (Prohibition, Prevention) Act, a number of legislation addressed internet crime to some extent:
The Economic and Financial Crimes Commission was given the authority to look into and punish a number of financial offences, such as computer fraud and piracy, under the EFCC Act.[11]

The Money Laundering (Prohibition) Act made it illegal to launder money and enforced stringent reporting requirements for major transactions in an effort to stop the funding of terrorism.[12]

The Criminal Code Act made theft and fraud by false pretences illegal, which applies to online scams even though it existed before the internet.[13]

Cybercrime charges are covered under the Penal Code Act, which is used in Northern Nigeria and addresses fraud, forgery, and counterfeiting.[14]

Act of 2013 on Terrorism (Prevention) (Amendment) with harsh punishments, including death sentences, it tackles cyberterrorism and terrorist finance, but in a more comprehensive manner.[15]

In order to prosecute cybercriminals, the Evidence Act of 2011 made computer-generated evidence acceptable in Nigerian courts.[16]

By clearly defining cybercrimes and outlining penalties, the Cybercrime Act of 2015 brought these initiatives together and strengthened Nigeria's cybersecurity laws.

4. Perceived Challenges

With an increasing number of attacks now taking place in cyberspace, Nigeria's security concerns have evolved with time. This development demonstrates the increasing sophistication of criminals, necessitating a corresponding modification of the nation's legal system and its implementation.[17] Targets frequently include a variety of industries, particularly the banking sector with its extensive data resources. Putting in place strong cybersecurity safeguards and enforcing the law correctly might help solve these problems.

Since cyberspace is still growing quickly, it is challenging to anticipate or stop illegal activity there. Cybercrimes, which include hacking into financial systems, gaining unauthorised access to passwords and private information, and even funding illicit activity, are increasing at a pace that is almost twice as high as traditional crimes. Nevertheless, under Nigeria's broader security framework, cybersecurity continues to be a low priority. Despite the existence of laws designed to prevent cybercrimes, their enforcement is still lacking because of inadequate agency cooperation

[11]Journal of Law and Criminal Justice June 2020, Vol. 8, No.1, pp.30-49
[12]Economic and Financial Crimes commission Establishment act (2004)
[13]Criminal Code Act
[14]Section 362 of the Penal Code Act
[15]Section 320 of the Penal Code Act
[16]Section 1 (b) of The Terrorism Act 2013
[17]https://www. recordedfuture.com

and a lack of readiness to handle breaches. To close these gaps, institutional structures must be strengthened and properly implemented.

Companies must also be proactive in protecting their data and infrastructure. However, many people take a lazy approach to defending themselves against cyberattacks, neglecting to spend money on cutting-edge IT systems or provide cybersecurity training to employees.[18]

Growing Numbers of Ponzi Schemes

Ponzi schemes have sprung up online since the COVID-19 outbreak, taking advantage of economic suffering and uncertainty throughout the world. In order to swindle people, criminals have resorted to the internet, frequently using complex financial schemes. In the well-known case of *Isaiah v JP Morgan Chase Bank*,[19] the bank was charged with permitting fraudulent transactions connected to a Ponzi scheme by doing nothing in the face of obvious warning signs. In a similar vein, fraudsters used Wells Fargo's infrastructure to channel illicit assets.[20]

People were more vulnerable during the epidemic due to the desperation brought on by job losses, poverty, and financial hardship. Millions of people were harmed, including hospitals and senior folks. For instance, on the pretence of providing medical equipment, scammers Parris and Santillo defrauded millions of dollars by offering fictitious investment returns. They then targeted hospitals and COVID-19 relief funds.[21]

Although they are not new, ponzi scams have become more widespread because of the internet. Widespread anxiety and financial hardship during the epidemic made people more vulnerable to these types of scams. There were several contributing factors:

Poverty: Since more than 40% of Nigerians are impoverished, many are lured to "get rich quick" scams in an attempt to escape their predicament. Progress has been sluggish, despite government officials' pledges to help millions escape poverty.

Lockdowns: During COVID-19, restrictions kept individuals indoors, which increased their vulnerability to fraudulent schemes and their usage of social media. Many resorted to fraudulent internet investments since they had few other options for earning money.[22]

Absence of Palliatives: Despite the government's assurances of assistance, the distribution of these packages was politicised, mishandled, or even hoarded in certain instances. Many Nigerians were left defenceless, which fuelled their eagerness to participate in fraudulent schemes, in contrast to nations that actively gave financial help to their populations.[23]

Weak Cyberspace Protection: Nigeria is one of the nations with the highest rates of cybercrime. Insufficient regulation makes it simple for dishonest actors to take advantage of the system. In one instance in Asaba, Delta State, Smart Alban Investment Company defrauded almost 1,000 investors out of millions of dollars, and the company's operator vanished.[24]

Most at danger are vulnerable populations, including the underprivileged and those without access to digital protection. Their exposure is increased by the digital divide, which is the difference

[18]The International Journal of Engineering and Science (IJES)

[19] 960 F.3d 1296 (11th Cir. 2020).

[20]https://www.natlawreview.com/article/ponzi-scheme-discovery-boom-may-follow-wake-worldwide-economic-contraction-case-law

[21]https://www.justice.gov/usao-dc/pr/georgia-man-pleads-guilty-charges-related-ponzi-and-covid-19-fraud-schemes

[22]Pakistan Social Sciences Review

[23]https://pubmed.ncbi.nlm.nih.gov/32685279/

[24]https://www.bbc.com/pidgin/tori-54677956

between those who have access to contemporary technologies and those who do not. Nigeria runs the danger of economic instability and a decline in institutional trust if these people are not protected. The reliability and equitable regulation of financial systems, ranging from banks to digital payment platforms, must be guaranteed to the public.[25]

Nigeria lacks the means and know-how to protect its online environment on its own. Therefore, utilising current commercial technology and implementing global best practices are crucial. Even if government and commercial organisations share accountability for safeguarding user data, carelessness still happens. Quick-fix patches or apologies following data breaches are insufficient; instead, accountability mechanisms and hefty fines should be implemented to enforce more robust protection.

It is often recognised that because laws are reactive rather than proactive, they frequently fall behind crimes. Nigeria already has a number of institutions that may help close this gap, but in order for them to do so, they need sufficient funding and authority. Furthermore, maintaining privacy necessitates striking a balance between education and enforcement. While institutions are held responsible for violations, citizens must be taught self-defence techniques.

The youthful, technologically literate populace of Nigeria poses both a risk and an opportunity. While some young people use technology for illegal purposes, others can be diverted towards creative endeavours and profitable endeavours. Effective policy execution, educational investment, and strategic planning are necessary to capitalise on this demographic advantage.

5. Conclusion

According to the report, digital technologies improve social institutions, healthcare, education, and economy, but they also pose threats that need to be carefully managed. Protecting individuals against cybercrimes and privacy violations is a legal and moral duty for both public and private entities. Nigeria has several organisations in place to improve cybersecurity regulation and enforcement, despite the fact that laws sometimes lag behind technical crimes.

Nigeria has to close the gap between rising cybercrime and inadequate cybersecurity measures if it is to prosper in the digital era. Better law enforcement, educational funding, safeguarding vulnerable populations, and utilising its young people as a resource are all part of this. Failing to do so may cause instability, erode social systems, and damage the economy. On the other hand, taking proactive measures will establish Nigeria as a safe and competitive digital country in the international marketplace.

[25]https://www.nairaland.com/6496590/sa-fx-ceo-mr-smart-alban