# Cyber Security and Data Protection as Tools for the Attainment of a Smart Nation: The Nigerian Example

**G. C. Omede, and *F. O. Okorodudu**

**Faculty of Sciences, Department of Computer Science, Delta State University, Abraka, Delta State, Nigeria.**

***Corresponding Author**

**DOI: https://doi.org/10.51584/IJRIAS.2024.905017**

**Received: 26 April 2024; Revised: 10 May 2024; Accepted: 14 May 2024; Published: 11 June 2024**

## ABSTRACT

Advancement in technology and globalization has led to newer forms of challenges such as the increased demand for individual data by governmental agencies and corporate bodies. This increased advancement and dependence on technology have made digital information to have a wider coverage than ever. This wider coverage of digital information comes with its attendant consequences of increased cybercrime and data right violation. This study takes an overview of the current state of cyber security and data protection policies and regulations in Nigeria in its quest to attain the status of a smart nation. The paper argues that the existing provisions for cyber-crime prevention and data protection regime is grossly inadequate to effectively protect individuals against abuse resulting from the processing of their personal data. The view of this study is based on the critical analysis of existing laws governing cyber-crime and data protection laws in Nigeria and the requirements for the attainment of a smart nation status. The study is of the opinion that the enormous volumes of digital traces containing personal data, if not well managed over the cyber world, could lead to their being exposed to unauthorized individuals with malicious intents. The study makes recommendations for the reform of the extant laws for the attainment of a smart nation status by Nigeria.

**Keywords:** cyber security, cyber-crime, data privacy, smart nation, Nigeria

## INTRODUCTION

In this digital age, any nation aspiring to attain the status of a smart nation must prioritize the privacy of information of its citizens. While the advancement in technology and globalization has created an environment where personal and organizational data can easily be assessed by anyone if they are not adequately protected, the undeniable fact that the lives of people have become interwoven with the continuous exchange of information and streams of data cannot be overemphasized [1] Consequently, more countries are beginning to take a stand on how best to protect personal data of their citizenry and reduce the occurrences of cybercrime. This is because, data is fundamental to the success of any society and economy and the protection of such data is critical towards the attainment of the status of a smart nation [2]

According to [3], cybercrime, which brings about cyber insecurity, is a type of crime that is committed by criminals who make use of the computer as a tool and the internet as a connection to reach a variety of objectives such as stealing of individuals' personal data without the consent of the individual. Cyber insecurity results from the wrongful application of internet facilities [4]. Cyber insecurity and data protection threats begin with the rapid increase in internet usage. This is because as the internet covers more ground, the risk of cyber insecurity increases [5] Staying shielded from cyber-attacks and having data protected from invasion requires that users are aware of the threats

Globally, as of 2003, the United States and South Korea were ranked as the countries with the highest number of cyber-attacks with 35.4% and 12.8% respectively [6]. This is despite the fact that these countries are highly advanced in relation to Nigeria. Sadly, studies by researchers have shown that 39.6% of Africans who use the internet are Nigerians [7]. With such a high percentage of internet users, Nigeria is yet to attain the status of a smart nation as the country is still struggling to enact relevant laws that would reduce the occurrences of cybercrime and protect the privacy of individuals and firms over the internet.

Nigerian cities, just like its contemporaries in most African cities, are poorly planned. The growth of Nigerian cities appear to be disorganized and frenzied with most cities laden with poorly regulated cyber world, poor infrastructure, limited transport services and scarcity of water and electricity. [8]. The idea of s smart nation is primarily a concept with no clear definition among academia and practitioners [9]. In general, a city or nation is said to be smart when traditional services and available infrastructure are made more flexible, efficient and sustainable through the use of information and communication technology (ICT) to the benefits of the residents of such cities or nation states [10]. From the foregoing, it is clear that cybercrime continue to grow and pose a serious threat to all sectors of the Nigerian economy.

## Overview of Cybercrime in Nigeria

The concept of cybercrime is a relatively new concept that is gradually growing as the internet continues to penetrate into every segment of the society. [4]. Cyber security has gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries like the United States. While cyberspace is the boundless space known as the internet, cyber security is the body of rule put in place for the protection of the cyber space. According to [11], cybercrime is any illegal act perpetrated in, on or through the internet with the intention to cheat, defraud or cause the malfunction of network devices, which may include computers, phones etc. in this sense, these illegal acts are those targeted at computer networks or devices including computer viruses, denial of service attacks, malware amongst others. The illegal acts originate from computer networks or devices that are independent of the computer network or device

Statistically, Nigeria was ranked as the 43rd country in Europe, Middle East and Africa (EMEA) and third among ten nations that commits cybercrime in the world. Consequent upon this ranking, the then president of Nigeria, Olusegun Obasanjo set up a National Cyber Security Initiative (NCI) in 2003. The efforts of the NCI after it set-up was unable to meet the growing rate of cybercrime in the country. Cybercrime thrives as a result of the lack of legal frameworks that can make it difficult to bring cyber criminals to book.

In a bid to nip in the bud the activities of cybercrime, the Cybercrime Act of 2015 was promulgated to address the menace of cybercrime in the country, However, like other similar Acts before it, the Act failed to totally arrest the ugly trend because of some gap in the Act and other factors that tended to exacerbate cybercrime in the country [12]

According to [4] cybercrime has become one of the main avenues for pilfering money and business espionage. According to Check point, a global network cyber security vendor, as of 2016, Nigeria was ranked as the 16th highest country in cyber-attack vulnerabilities in Africa [13]. Acts of cybercrime have given Nigeria a very wrong image in the international community as Nigerians are known to be high class perpetrators of cybercrimes globally. The activities of internet fraudsters has been on the increase in the last decade despite efforts by relevant bodies and agencies [5]. The internet has had a huge impact on various sectors of the Nigerian economy. However, most of these sectors such as the banking sector, the education sector, the social media, and the e-commerce sector are finding it difficult to cope with the activities of cyber criminals which have become a thorn in their flesh.

In the banking sector for instance, with the implementation of the Bank Verification Number (BVN) in 2015 by the Central Bank of Nigeria, activities of fraudsters have become prevalent. Such acts as identity theft (phishing), theft of bank cards, cyber theft/banking fraud, internet order fraud etc. have become the order of the day. Use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS or at the ATM is now a possibility. According to the Federal Bureau of Investigations (FBI), a method known as ATM skimming which involves the placing of an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine [14] is now a common occurrence

Also, cybercrime in the social media sector is now rift with the increase in the use of social media platforms such as Facebook, Twitter, WhatsApp, Instagram, LinkedIn and the likes. Using the social media allows a person to communicate with friends without restriction [15]. These social media platforms have become a handy tool for cyber criminals to hijack and demand money in turn for releasing personal social media page. These hacking have occurred in Facebook, Twitter, WhatsApp, Instagram and the likes. These fraudsters go as far as sending messages from authorized page to friends and families requesting for money or other forms of assistance. Such is the extent to which cybercrime have become a nuisance to the society

Wrong value system has been identified as one of the major causes of cybercrime in Nigeria [16]. [17] identified unemployment, quest for wealth, lack of strong cybercrime laws and incompetency on the part of security on personal computers as the bane of cybercrime in the country.

**Data Protection Framework in Nigeria**

As a signatory to the United Nations Declaration on Human Rights, (UDHR) in 1948, the law on the right to the protection of one's privacy from intrusion by the state as enshrined in Article 12 of the charter is binding on Nigeria. However, this does not address the issue of how to protect individuals' data. While privacy is a fundamental human right guaranteed by the 1999 Constitution of the Federal Republic of Nigeria, a comprehensive data protection legislation is yet to be enacted as the existing framework that apply to personal data protection are from the broadly framed Section 37 of the Constitution which provides that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected" [18]. Some vital issues were raised concerning this constitutional provision as [19] stated that beyond the constitutional provision, there is no machinery for enforcement as Nigeria does not have specific privacy laws but the right to privacy that is guaranteed by the constitution. There is also the argument that the law is discriminatory against non-citizens since it only stated that the 'privacy of citizens" [20]

Several efforts have been made to enact laws that would make adequate provisions for data protection. Such draft bills as the Cyber Security and Data protection Agency bill 2008, the Electronic Fraud prohibition Bill 2008, the Nigerian Computer Security and protection Agency Bill 2009 and the Computer Misuse Bill 2009 that would have addressed cybercrime and data protection issues in Nigeria have not been passed into law.

The Freedom of Information Act of 2011 which was enacted to make public records and information freely available, provide for public access to records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy etc. cannot be regarded as a data protection legislation as the provisions are not comparable to what is obtained in developed societies.

In September, 2013, the National Information Technology Development Agency Draft Guidelines on Data protection was released. The document contained guidelines which were issued in pursuance of the Act that established the National Information Technology Development Agency (NITDA). Section 6 of the Act mandates that the agency shall among other things, develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transaction as an alternative to p**a**per based methods in government and other sectors. The claim to data protection by the NITDA Act does not hold much water as the provisions of Sections 6, 17 and 18 does not conform or relate to any known data legislation in the world.

In 2014, the African Union Convention on Cyber Security and personal Data protection 2014 was enacted.

The convention is an international legal instrument entered into by the members of the African Union (AU), including Nigeria. the goals of the convention, among others, is to address the need for a harmonized legislation in the area of cyber security among member states and the establishment in each state, a mechanism capable of combating violations of privacy that may be generated by private data collection, processing, transmission, storage and use. However, like most other treaties entered into by Nigeria, the convention is yet to come into force in Nigeria as it requires an enactment from the National Assembly for it to come into law.

**Nigerian Cybercrime and Data Protection Statistics.**

There seems to be an alarming upward trend in cyber breaches and assaults in Nigeria, according to the available statistical data gotten from global cybersecurity firms; between 2020 to 2023. An overwhelming majority of Nigerian firms, 71% to be exact, were hit by ransomware attacks in 2020 and 2021. Furthermore, 82,000 data breaches were detected in Nigeria in the first quarter of 2023, suggesting that cybersecurity remains a concern in the nation [21].

The use of predictive modeling allows us to extend this tendency and foretell when cybercrime would occur in Nigeria. The probability of cyber breaches and assaults in the future may be estimated using a model that takes into account both past data and present trends.

Predictive modeling should take into account factors such as the growing number of digital transactions in Nigerian companies, the fact that many firms do not have sufficient cybersecurity safeguards in place, and the fact that cybercriminals are constantly adapting their techniques. Based on our analysis of these patterns and causes, we can predict that cybercrime events in Nigeria would continue to rise until there are substantial improvements to cybersecurity measures.

Organizations in Nigeria must prioritize the development of strong cybersecurity plans, the education of their employees, and the continuous updating of their security systems in order to counteract the anticipated rise in cybercrime in the country. There is a correlation between the prevalence of cyberattacks and the lack of government action or policy to raise cybersecurity awareness or ensure compliance with data protection laws.

## CONCEPT OF A SMART NATION

The concept of what a Smart Nation or City is, is a subject that has been of interest to researchers globally. Even though the smart nation concept is seen by some as a marketing tool, the concept varies from nation to nation or city to city depending on the level of development and desire for improvement, coupled with the resources available to the residents of such nations or cities [10]. A smart nation brings with it huge opportunities. However, most African countries, including Nigeria are lagging behind in smartening their nations due to constraints such as the non-availability of finance, skills, technology and energy resources [8].

Consequently, a smart nation according to [10] is a nation that interconnects its physical, social and business infrastructure to fully utilize the collective intelligence of the city. [22] And [23] have also implied in their definition of what a smart nation is that it is one which has embraced information technology and other measures to improve the quality of life of its citizenry as well as in the efficiency of the nation's operations and services. The idea of a smart nation is associated with the use of advanced and innovative technology together with hard infrastructure and social capital to efficiently drive sustainable economic growth, competitiveness, prosperity and a better life for its people.

A smart nation is one that has keyed into the idea of a new industrial revolution known as the Fourth Industrial Revolution (FIR). This FIR leads nations to an era in which the world is impacted by exponential disruptions of a magnitude higher than the three previous revolutions. In other words, the fourth revolution is driven by 36 novel areas of innovation in IT, such as new Robotics systems, Drones, IoT (Internet of

Things), Automated Vehicles or Driverless Vehicles, Cloud Computing, Artificial Intelligence, Nano Technology, amongst others. With the FIR, new functional societal endeavours such as Smart Homes, Smart Transport, Smart Buildings, Smart Industries, Smart Finance, Smart power Grids, Smart Schools etc. have become a societal norm.

Thus, a country that desires to attain the status of a smart nation must be ready to enact relevant laws that would address all observed loopholes to the attainment of such a status. In essence, for Nigeria to attain the status of a smart nation, she must make effort to make laws that would make adequate provision for the protection of the data of its people and make the internet more conducive.

## THE SINGAPORE EXAMPLE

Currently, Singapore is ranked as the worlds' smartest nation [24] and [25]. Since 2014 when the Singaporean prime minister launched the smart nation program, the nation has been on the ascendency more than any other nation of the world. The program saw the launch of unspecified sensors and cameras that were deployed across the nation to monitor everything, from its cleanliness to the traffic control system [26]. With the launched program, Singapore became a digital town, with virtually everything and everybody under watch. This of course grew the economy of the country.

Singapore's ambition to become a smart nation was built on a secure foundation. The nations' cyber security agency (CSA) was empowered to drive cyber security level through the adoption of a security-by-design approach in the development of the national digital infrastructure. The adoption of the approach was critical because any disruption of services or loss of sensitive personal data could cause malicious cyber activity that would erode trust in the national digital infrastructure and digital government services. Also, the CSA was designed to work with critical information infrastructure owners to strengthen the resilience of their networks to cyber-attacks and minimize the risk of disruptions to the delivery of essential services across the Singaporean nation. Further, the CSA works with the business associations to prioritize cyber security and encourage their members to tap on its cyber security expertize and adoption of good cyber security practices. The CSA was also designed to reach out to the general public to promote basic cyber hygiene practices such as the need to use strong passwords and two factor authentication and to be aware of phishing emails

## FINDINGS OF THE STUDY

Based on the findings of this study as to the extent to which Nigeria have gone in attaining a smart Nation status in relation to cyber security and data protection, the study submits that Nigeria is still very far from attaining a smart nation status because of the following reasons:

1. Cybercrime is a problem that is rooted in technology

2. There is no major agency of government or non-government that is responsible in protecting citizens against cybercrime or even where to report incidence of cybercrime.

3. Lack of legal framework and the required skill by law enforcement agents to handle cybercrime

4. Lack of transparency in the processing of personal data. In the context of the law, an individual has the right to be told if their data is being processed and what it is to be used for. The processing operation should not be carried out in secret and should not have any negative effect on the individuals. Sadly, this is not so in some cases as individual information are disclosed to third parties.

5. Lack of data security and the risk of a personal data violation. Data security is a key requirement in data protection. Due to the relaxed laws on cyber security in Nigeria, there is no positive obligation imposed on online platforms in Nigeria to take necessary data security measures to protect individual

personal data. Consequently, there is the risk of the loss of control of personal data

6. Lack of adequate consent. For consent to be freely given, it is required that individuals are adequately informed of what and how their personal information is to be used. However, in Nigeria and most developing countries, individuals are not adequately informed in order for them to provide consent for a specific purpose.

7. Children are exposed to privacy risk online as they unknowingly consent to some requirements online due to the appealing nature of their visual content without knowing the implications of their actions

## CONCLUSION

Cyber security and data privacy invasion threat is a global issue. Any nation seeking to become smart in its way of doing things must first adequately tackle the menace of cyber insecurity and data privacy invasion. A sustained national effort is needed to systematically educate and promote the pervasive use of technology among Nigerians to reduce the menace. In the effort to create a more secure online environment and take actions against cyber criminals, relevant laws must be made to govern the freedom, creativity and innovation of internet users. In doing this, effort must be made to not impede on the rights of citizens to create, interact and roam on the internet. Thus, a more informed and thoughtful approach that will put into consideration all the elements needed to achieve efficiency and the long term sustainability of Nigeria is advocated. A city is said to be smart if it has one or more smart components such as smart technology, smart transportation, smart economy etc. A unique way to attaining smart nation status is through smart technology. Smart technology involves amongst others, the adequate protection of the rights of citizens either online or offline. It is through the adoption of advanced technologies with the enactment of relevant laws that the cyber world would exponentially allow a nation to rapidly attain the status of a smart nation.

## RECOMMENDATIONS

For Nigeria to attain the status of a smart nation, the enactment of a data protection Act that will contain data protection principles consistent with those obtainable with international standards is very relevant. The Act should be holistic and must be applicable to the private and public sector, to actualize these there should be collaboration and partnerships among the industries, academia, Government agencies and the civil society.

This will tackle the challenges of smart nation by providing adequate funding, regulatory issues, and training across all sectors to eliminate digital literacy and enforce long term sustainability which will embody all stakeholders

## REFERENCES

1. European Union Agency for Fundamental Rights (2010). Data Protection in the European Union: The Role of National Data Protection Authorities. Luxembourg: Publications Office of the European Union. EMC. Global Data Protection Index. (December):11–21, 2014.
2. Maitanmi, O. Ogunlere,S. andAyinde S. (2013), *Impact of Cyber Crimes on Nigerian Economy*, The International Journal of Engineering and Science (IJES), vol. 2(4), 45–51.
3. Omodunbi B.A., Odiase P.O., Olaniyan O.M and Esan A.O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, Volume 1, Issue 1, September 2016, 37 -42
4. Okorodudu F.O and Okorodudu P.O. (2017). Cyber Security and Digital Privacy: An Imperative for Information and Communication Technology and Sustainable Development in Nigeria. International Journal of Research, vol. 4, issue 3, March, 2017, 412-421

5. Lakshmi P. and Ishwarya M. (2015), *Cyber Crime: Prevention & Detection*,” International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).
6. Hassan, A. B. Lass F. D. and Makinde J. (2012) *Cybercrime in Nigeria: Causes, Effects and the Way Out*, ARPN Journal of Science and Technology, vol. 2(7), 626 – 631.
7. Woherem E,E and Odedra-Straub M. (2017). The Potentials and Challenges of Developing Smart Cities in Africa**,** Circulation in Computer Science. 2, No.4, pp.: (27-39), May 2017
8. Saraju, E.K and Mohanty, P. (2016) “Everything you wanted to know about smart cities: The Internet of things is the backbone,” *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60-70, 2016.
9. Halimi, H. (2016) “African smart cities: Potential and Pitfalls,” 28 October 2016. [Online]. Available:http://www.urbanafrica.net/urban-voices/african-smart-cities-potential-and-pitfalls/. [Accessed 05 December 2019].
10. Augustine C. Odinma, MIEEE (2010): *Cybercrime& Cert: Issues & Probable Policies for Nigeria*, DBI Presentation, Nov 12.
11. Umejiaku N.O and Anyaegbu M.I. (2016). Legal framework for the enforcement of cyber law and cyber ethics in Nigeria.
12. Ewepu G, (2016) *Nigeria loses N127bn annually to cyber-crime* — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/ Retrieved Jan. 07, 2019.
13. Michael A.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz, vol. I WCECS 2014, 22–24.
14. Longe, O. B, Chiemeke, S. (2008): *Cyber Crimeand Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4*
15. Izuogu, C.E. (2018). *Personal data* protection in Nigeria. World Wide Web foundation and Paradigm initiative
16. Kusamotu, A. ‘Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46’ (2007) 16/2 *Information & Communications Technology Law* 149–59 at 154.
17. Abdulrauf, L.A. (2016). The legal protection of data privacy in Nigeria: Lessons from Canada and South Africa, unpublished Ph.D. thesis, University of Pretoria.
18. Omoleye Omoruyi, “ Nigeria sees 64% increase in data breaches, recording an outstanding 82,000 episodes in Q1 2023”, <https://technext24.com/2023/05/23/nigeria-records-82000-data-breach-in-q1/>, accessed on September 18, 2023.
19. Fitsilis P. (2014). ExPloring architectural and organizational features in smart cities. In 16th International Conference on Advanced communication Technology, Korea, IEEE, pp.190 – 195
20. Samsi J.A. (2015). “Smart city architecture: vision and challenges”. International Journal of Advanced Computer Science and Applications (IJACSA), col 6, no 11, pp. 246 – 225.
21. Juniper Research. (2016). Singapore name ‘Global smart city 2016’ sourced online from https://www.juniperresearch.com/press/pressaccessed January, 7, 2019
22. Buntz B. (2016). The World’s smartest cities. Sourced online from http://www.ioti.com/smart-cities/world-a-5-smartest-cities [accessed 77 January 2019
23. Purnell N. (2016) Singapore is taking the ‘Smart City” to a whole new level’ sourced online from http://www.wsj.com/articles/singapore-is-taking-the-smart-city-to-a-whole-new-level-1461550026[accessed 77 January 2019