

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

Legal Frameworks for Cybersecurity in Nigeria - Adapting The Fourth Industrial Revolution

Ibitamuno, Pamela Victor

CSEAN Administrative Officer/Cybersecurity Lawyer

E-mail: pamelavictoribitamuno@gmail.com

Phone: +2348146170040

ABSTRACT

In this article titled "The Legal Framework for Cybersecurity in Nigeria: Adapting the Fourth Industrial Revolution," the author explores the legal landscape governing cybersecurity in Nigeria in the context of the Fourth Industrial Revolution (Industry 4.0). The Fourth Industrial Revolution is characterized by the integration of digital technologies such as the Internet of Things, cyber-physical systems, and cloud computing, which has created a hyper-connected system. As this revolution progresses, cybersecurity becomes critical to ensuring the security of the digital space. The article emphasizes the need for the legal framework to evolve in line with societal changes brought about by the Fourth Industrial Revolution. Nigeria's legal framework for cybersecurity must adapt to the challenges posed by the rapid integration of digital technologies and cyber-physical systems in our daily lives. A robust and adaptive legal framework is essential to safeguard national security, protect personal data, and foster a secure digital ecosystem conducive to economic growth and technological advancements. This Article also calls out to the stakeholders, policymakers and the Government of Nigeria to take the necessary steps required for signing the Malabo Convention, as Nigeria is yet to sign the African Union Malabo Convention. This is vital in our steps to adapt to the Fourth Industrial Revolution.

Keyword: Proactive Approach, Security Challenges, Cloud Migration, Security, Risks, Models

Proceedings Citation Format

Ibitamuno, P.V. (2023): Legal Frameworks for Cybersecurity in Nigeria - Adapting The Fourth Industrial Revolution. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 97-104. <https://www.csean.org.ng/>. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P12

1.. INTRODUCTION

Legal Framework includes the comprehensive legal system for a particular jurisdiction established by any combination of the following: a constitution; primary legislation enacted by a legislative body which has the authority in respect of the jurisdiction; subsidiary legislation made by authorities authorized by the primary legislation for such jurisdiction; policies,

practices, or procedures implemented by authorities authorized by the primary legislation for such jurisdiction; and legal precedent and customs applied by the courts (Law Insider, n.d). The Legal Framework for the regulation of cyber security in Nigeria refers to all the legislation, policies, practices, or procedures implemented by authorities authorized by the primary legislation for such jurisdiction; and legal precedent and customs applied by the courts for the sole purpose of regulating the cybersecurity landscape in Nigeria.

The Fourth Industrial Revolution looks promising. Although, it poses some dangers if not properly regulated. This revolution is happening so speedily forcing individuals to have a rethink on how countries can develop, how organizations can create value, what it means to be human and how humanity can be helped. The Fourth Industrial Revolution is not just a technology-driven change. It is an opportunity to help everyone, including leaders, policy-makers and people from all nations. The question is “How do we ensure cybersecurity in this Fourth Industrial Revolution? How can policy makers in Nigeria mitigate potential dangers? How can Nigerian laws adapt to the current change. The author aims to examine the existing legal framework for cybersecurity in Nigeria and identify the necessary adaptations to for the cybersecurity laws in the Fourth Industrial Revolution era.

2. THE LEGAL FRAMEWORK FOR CYBERSECURITY IN NIGERIA

Nigeria has recognized the importance of cybersecurity through several legal and policy initiatives. Key cybersecurity laws in Nigeria include the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 and the National Information Technology Development Agency (NITDA) Act 2007. Additionally, the Nigeria Data Protection Regulation (NDPR) of 2019 provides guidelines for data protection and privacy.

The Legal framework for cybersecurity in Nigeria includes;

3.1 The Cybercrimes (Prohibition, Prevention and Punishment) Act 2015: The Cybercrimes (Prohibition, Prevention, and Punishment) Act of 2015 was passed and went into effect on May 15, 2015. It gives effect to the 2011 ECOWAS Directive in fighting cybercrime. The Act establishes a uniform and comprehensive legal, regulatory, and institutional framework in Nigeria for the prohibition, detection, prosecution, and punishment of cybercrime. The legislation also protects essential national information infrastructure, promotes cyber security, and protects computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights. The Act charges the offices of the National Security Advisor (NSA) and the Attorney-General of the Federation (AGF) with coordinating its enforcement and creates the multi-agency Cybercrime Advisory Council (the Council) and the National Cyber Security Fund (the Fund) to be overseen by the NSA. Section 38 of the Cybercrime Act 2015 requires service providers to keep all traffic data and subscription for a period of at least 2 years. Failure attracts a fine of 7million naira. Section 39 requires service providers, upon a court order, to assist competent authorities with the collection or recording of content or traffic data. Section 40 requires service providers to assist law enforcement agencies in identifying offenders. The Act prescribes 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.

- 3.2 **The Criminal Code Act 1990:** The Criminal Code Act 1990 criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although, cybersecurity and cybercrime is not mentioned in the Act. If a cybercrime involves stealing, it is punishable under the Act. Chapter 38 of the Act deals with obtaining property by false pretenses (cheating). Section 419 states that any person who by false pretense, and with the intent to defraud, obtains from any other person anything capable of being stolen, or induces the person to deliver to any person anything capable of being stolen, is guilty of felony, and is liable to imprisonment for 3 years. This provision in addition with the provisions of the Cybercrimes Act punishes offenders who defraud victims over the internet, thereby committing cybercrime.
- 3.3 **National Cyber Security Framework of NITDA 2019:** This framework targets at making Nigeria a cyber-resilient State, highlighting the functions the organization has to perform to overcome negative consequences of cyber-attacks, analyze global information assurance frameworks that could safeguard the organizations in cyberspace and create collaboration for organizations seeking to benefit from the intelligence of other organizations.
- 3.4 **The Nigeria Cybersecurity Strategy 2014:** It established the National Computer Emergency Response Team (CERT) and introduction for a roadmap for implementing detective, preventive and response capabilities to deal with cybercrime activities. The Nigerian Computer Emergency Response Team (ngCERT) was founded under the National Security Adviser's Office. The ngCERT's major objective is to manage the risks of cyber threats in Nigeria's cyberspace and efficiently coordinate incident response and mitigation plans to proactively prevent cyber-attacks against Nigeria. It is situated under the Office of the National Security Adviser. The primary functions are as follows: to develop a common situation awareness platform, to properly handle and coordinate the management of a national-interest incident, to aid in the implementation of the National Cybersecurity Policy and to function as the worldwide point of contact for all Internet security incidents in Nigeria
- 3.5 **The Economic and Financial Crimes Commission Act, 2000:** The Act provides for the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, computer credit card fraud, futures market fraud. It also provides for the examination of all reported cases of economic and financial crimes
- 3.6 **Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBS) and Payment Service Providers (PSPS) ("The Guideline"),** which became effective in January 1, 2019
- 3.7 **Other Legal Frameworks include;** The Nigerian Communication Act 2003, The Evidence Act 2011, National Broadcasting Commission Act, The Terrorism (Prevention) (Amendment) Act 2013, The National Identity Management Commission Act 2007.

4. ANALYSIS OF THE EFFECTIVENESS OF THE CURRENT CYBERSECURITY LAWS

While Nigeria's existing cybersecurity laws are commendable, they face challenges in keeping up with the rapidly evolving cyber threats. The Cybercrimes Act, enacted in 2015, may need updates to address the recent advancements in cybercriminal activities. The Cybercrime Act, which is the law that is assumed to effectively tackle cybercrime in Nigeria, was enacted in 2015. Cybercriminals have evolved and found various ways to carry out cybercriminal activities which the law does not provide for. Sadly, most Nigerian judges are not able to interpret these laws and apply it to complex technological cases that have arisen.

5. CHALLENGES IN DIGITAL EVIDENCE AND ADMISSIBILITY OF DIGITAL EVIDENCE BY NIGERIAN COURTS OF LAW

The Nigerian Evidence Act (2011) provides for digital evidence. The Act refers to it as 'computer generated evidence'. Computer generated evidence are special and so they require special analysis by legal practitioners, judges and experts. 'Evidence' has been defined in the Black's Law Dictionary to mean a testimony, documents and tangible objects that tends to prove or disprove the existence of an alleged fact. Digital Evidence processed by emerging technologies ought to be used as evidence. However, it may be considered inadmissible by courts or considered to be unreliable. This may be because it is obtained without authorization or lacks authenticity.

Some of the challenges experienced with digital evidence are;

- 5.1** Digital evidence obtained from a storage media is likely to be large in file.
- 5.2** Extracting the right piece of evidence needed is a big challenge.
- 5.3** Not all portions of evidence can be collected manually. Certain evidence in the form of logs in the systems can reveal very little information about the crime. Further, more information has to be collected by employing the appropriate forensic tools. Therefore, a forensic investigator who is professionally sound should be involved in the collection of evidence. This is not always the case in Nigeria.
- 5.4** The digital evidence collected should be able to completely map a crime scene which otherwise would make it worthless and difficult in proving the crime.

While Nigeria's existing cybersecurity laws are commendable, they face challenges in keeping up with the rapidly evolving cyber threats. The Cybercrimes Act, enacted in 2015, may need updates to address the recent advancements in cybercriminal activities. Section 84 of the Evidence Act provides thus; (1) In any proceedings, statement contained in a document produced by a computer shall be admissible, as evidence of any fact stated in it, which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question. It is clear that there can only be an admissibility of computer generated evidence if the condition spelt out in Section 84(2) of the Act is fulfilled. What are the conditions Section 84(1) of the Act is talking about? Section 84(2) provides; the conditions referred to in subsection (1) of this section are; a) that the documents containing the statement was produced by a computer during a period over which the computer was used regularly to store or process information for the purpose of

any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual; b) that over that period, there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind contained in the statement of the kind from which the information so contained is derived; c) that throughout the material part of that period, the computer was operating properly or if not, that in any respect in which it was not operating properly, or was out of operation, during that part of that period, was not such as to affect the production of the document or the accuracy of its contents and; d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities. It must be understood that Section 84 of the Act, in providing that in any proceeding, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it, of which direct oral evidence would be admissible, put the admissibility of a document produced by a computer under the rules pertaining to oral evidence from Sections 125-130 of the Evidence Act, 2011.

The limitations to the admissibility of digital evidence are as follows: Acquisition of volatile data (live forensics) is tough and very difficult to recover; Digital evidence is more susceptible to tampering and alteration. In some cases, digital evidence is deemed as tampered evidence. Though hashing is used to or the integrity of digital evidence, admissibility of computer-generated electronic records cannot be relied upon solely and can be used as corroborative evidence. The prosecutor and the court must be abreast with the ongoing legal and technological advancements as electronic evidence has substantial impact during trial. Thus, there is need for Nigeria to devise a mechanism for ensuring the veracity of contents of electronics has to be discussed with the court prior to commencement of trial.

6. ADAPTING TO THE FOURTH INDUSTRIAL REVOLUTION LANDSCAPE

The Nigerian Government and the general public have justified concerns over bias, privacy, accountability, transparency and the complexity of the emerging technologies of the Fourth Industrial Revolution. These emerging technologies also come with some negative consequences arising from the usage, such as privacy issues, security vulnerabilities threatening the privacy of emerging technology users, using emerging technology for unlawful surveillance (such as the wireless non-contact use of radio-frequency electromagnetic fields to transfer data with the aim to automatically identify and track tags attached to objects; if this is installed without the knowledge of the receiving person, the person can become a lifelong object of surveillance) Dimov (2016): unlawful use of beacons to allow criminals identify behavioral patterns of potential victims, unlawful collecting of personal data through social networking platforms and unlawful use of radio-frequency identification chips. Here are some key aspects of how the legal framework in Nigeria can adapt to the Fourth Industrial Revolution in the context of cybersecurity:

1. **Comprehensive Cybersecurity Legislation:** Nigeria should consider enacting a comprehensive cybersecurity legislation that specifically addresses the emerging technologies and unique risks associated with the Fourth Industrial Revolution. This legislature must address the recent advancement in cybersecurity that is not addressed in the Cybercrime Act (2015).

2. **Cybersecurity Standards and Best Practices:** The legal framework should promote the adoption of cybersecurity standards and best practices across industries. Establishing guidelines for the secure implementation and use of emerging technologies will help organizations protect themselves from cyber threats.
3. **Strengthening The National Computer Emergency Response Team:** The National Computer Emergency Response Team or any designated cybersecurity agency in Nigeria should be adequately empowered, funded, and staffed to effectively coordinate responses to cybersecurity incidents related to Fourth Industrial Revolution technologies.
4. **Public-Private Partnerships:** Collaboration between the government, private sector, academia, and civil society is crucial to address cybersecurity challenges effectively. Public-private partnerships can enhance information sharing, joint threat analysis, and capacity-building initiatives.
5. **Capacity Building and Training:** Nigeria should invest in cybersecurity education and training programs to develop a skilled workforce capable of handling cyber threats posed by emerging technologies.
6. **Research and Innovation:** Encourage research and innovation in cybersecurity technologies and solutions to address the evolving cyber threat landscape. Supporting local talent and startups can lead to the development of innovative cybersecurity solutions.

7. WHAT POLICY MAKERS IN NIGERIA CAN DO TO ADAPT TO THE FOURTH INDUSTRIAL REVOLUTION

Policy Makers in Nigeria can;

1. Develop emerging technology standards for children.
2. Create actionable guidelines to educate, empower and protect children and youths.
3. Bring Technology Companies, Governments, NGOs, Civil Services, and Academic Institutions together to accelerate the adoption of responsible technologies in the Fourth Industrial Revolution in the interest of the public.
4. Strategize measures for the Evidence Act 2011 to reflect the current technological changes with regards to the admissibility of online generated evidence.
5. Strategize measures to make the Cybercrime Act 2015 reflect the current changes and to be more enforceable.

8. TRAINING OF JUDGES TO INTERPRETE AND APPLY THE LAWS TO FIT THE EVOLVING CHANGE

The advancement of technology and the emergence of the Fourth Industrial Revolution present a significant need for trained judges in Nigeria to handle cases related to cybercrime, cybersecurity, and technology. Judges must be well-equipped to navigate hybrid hearings and understand courtroom cybersecurity. They should also be capable of interpreting court cases involving digital evidence and online interactions, as well as making decisions regarding criminal justice algorithms. Misinterpretation of laws and evidence by judges can have severe consequences for all parties involved. To address this, it is essential to hold mandatory conferences for judges that focus on technology topics, enabling them to become conversant with technological issues. Judges should also have a mandatory duty of 'tech compliance,' obligating them to be knowledgeable about technological matters.

To protect judges and judicial employees from social engineering tactics employed by cyber-attacks, they can utilize part of their Continuing Legal Education (CLE) to undergo computer security training. During judicial conferences, judges should be exposed to technology topics, such as courtroom technologies and cybersecurity. While they don't need to be experts, having a basic understanding is crucial. A judge who is tech competent can better interpret how existing laws apply to cases involving technology. Furthermore, judges need to understand best practices for keeping their systems secure from cyber-attacks. Tech-savvy judges can also be vigilant in detecting disruptive effects from jurors who engage in online misconduct, such as researching parties and issues online or communicating with third parties through social media. This issue has garnered considerable attention, leading many jurisdictions to update their jury instructions and admonishments to address this threat. In the Digital Age, judges must be aware of the potential damage jurors' online activities can cause to the integrity of judicial proceedings and the presumption of fairness and impartiality in those proceedings.

Therefore, equipping judges with technological knowledge is essential for the effective and fair handling of cases involving emerging technologies and cyber-related matters. Judges do not have to be experts; they just have to be conversant. (Jeff Schrade n.d). A judge who is tech competent will not only be aware of the potential for lawyers and staff to engage in online misconduct but will also be vigilant in detecting the disruptive effects of jurors who threaten the integrity of the justice system through various forms of online misconduct. Such misconduct consists of jurors “researching” the parties and issues online and communicating with third parties—or even litigants themselves—via social media platforms. Sisak (2014). This is a persistent issue that has been the subject of considerable attention, including scholarly articles. Browning J (2020). It has also led to many jurisdictions revising or updating their jury instructions and admonishments to address this threat from inside the jury box. Amy J. St Eve et al (2014 pp64,86-89).

9. LAW AS A TOOL OF SOCIAL ENGINEERING

Roscoe Pound's social engineering theory posits that law is a powerful instrument capable of shaping and changing society's behavior. According to Pound, the purpose of law is to serve society, and therefore, society itself shapes the law to meet its needs. The law should function as a means of bringing about social change rather than acting as a hindrance. The essence of laws lies in making society more adaptable and responsive to changes in its ideals and principles. Laws are designed to prevent conflicts and disputes and enable the society to progress and grow in all aspects. In the context of Nigeria, the law is considered the last hope for the common man in restoring order and driving societal change and growth. When it comes to Cybersecurity, the legal framework must be oriented towards progressive change and growth. The law should be flexible and able to adapt with the evolving society and advancements in various aspects of life. A well-crafted law does not stifle innovation; instead, it regulates and accommodates innovations to ensure a balanced and secure society.

10. NIGERIA SIGNING THE MALABO CONVENTION: A STEP TO ADAPTING THE FOURTH INDUSTRIAL REVOLUTION

Nigeria is yet to sign the African Union Malabo Convention. Africa has taken steps in her efforts to address issues of cybersecurity and data protection, thereby creating a comprehensive legal framework for electronic commerce, data protection, and cybercrime and cybersecurity on the continent. Nigeria is encouraged to sign the Malabo Convention and ratify it as this would be a huge step in adapting to the Fourth Industrial Revolution.

11. CONCLUSION

The Fourth Industrial Revolution brings transformative technological advancements to Nigeria but also exposes the nation to complex cybersecurity threats. A robust legal framework for cybersecurity is essential to protect national interests, preserve personal data, and facilitate a secure digital environment for socio-economic growth. By adapting its legal framework to the challenges posed by the Fourth Industrial Revolution, Nigeria can embrace the opportunities presented by the digital era while mitigating the risks associated with cyberspace.

REFERENCES

1. Alice Corp. v CLS Bank International, 573 U.S., 134 S. Ct. 2347 (2014)
2. Black, H. C. (2014). Evidence. In Black's law dictionary (10th ed., p. 642). Thomson Reuters
3. Cybercrime (Prohibition, Prevention, etc) Act 2015. (2015). Federal Republic of Nigeria Official Gazette, 102(94), A2015
4. Desai, D., Khan, N., 'Cyber Crime: A New Species of Crime', 8 Supremo Amicus 86 (2018).
5. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors (2007)
6. Dimov, D (2016, February 24): Legal Issues of New and Emerging Technologies. Infosec <https://resources.infosecinstitute.com/topic/legal-issues-of-new-and-emerging-technologies/>
7. Eva A. Vincze, 'Challenges in Digital Forensics', 17 POLICE PRAC. & Res. 183 (2016)
8. Kraak, M., Ormeling, F., 'Cartography, Third Edition: Visualization of Spacial Data', Guilford Press 2011
9. LawTeacher. November 2013. Relevancy and Admissibility of Electronic Evidence. [online]. <https://www.lawteacher.net/free-law-essays/commercial-law/relevancy-and-admissibility-of-electronic-lawessays.php?vref=1>
10. NIST Computer Security Resource Center (n.d) Cybersecurity. <https://csrc.nist.gov/glossary/term/cybersecurity>
11. The Malabo Roadmap (2022, September)
12. Viyo O., (2015) 'Law: A strategic tool for social engineering" <https://9jalegal.com.ng/law-a-strategic-tool-for-social-engineering/>
13. Ugoagba, C. (2023, February) Forensics and Digital Evidence in Cybercrime Investigation. Researchgate ² https://www.researchgate.net/publication/368692167_FORENSICS_AND_DIGITAL_EVIDENCE_IN_CYBERC_RIME_INVESTIGATION
14. World Economic Forum (2023) Fourth Industrial Revolution. Weforum <https://www.weforum.org/focus/fourth-industrial-revolution>