

ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES: ASSESSING NIGERIA'S PREPAREDNESS FOR ITS LEGAL IMPLICATIONS THROUGH HER CURRENT LEGAL FRAMEWORKS

IFEANYI MAXWELL OKOBIA, ESQ^{*}
ENEMHINYE EHIGIATOR, PhD^{**}

Abstract

The world is in a digital age as technologies shape the new way of life. Artificial intelligence and other emerging technologies now dominate all spheres of life and in most instances, have replaced human labour and have done so efficiently and effectively. Technologies have also found a way to make the performance of certain activities faster and seamless. It has undoubtedly come at a cost. The risks are as abundant as the benefits; this is where the legal and institutional frameworks come in to checkmate these negatives and limit these emerging technologies to a large extent its benefits only. The obvious risks include data rights violations, cybercrimes, cyber money laundry and privacy breaches. In most countries including Nigeria, there exists Data Protection Laws and other legal frameworks to regulate the impact of technologies on citizen's rights and lives. These laws are what the researchers herein seek to assess to uncover its sufficiency or otherwise in the light of the ever emerging and evolving technologies. In a rapidly technologically advancing society, the law-making bodies have their work cut out in meeting up with enactment of laws and possibly making room for future eventualities. AI and other emerging technologies is also a bundle of powerful resources which in no distance time will rank well above natural resources currently sustaining countries of the world like Nigeria. However, the absence of proper and sufficient legal frameworks to regulate the efficient transition to this new world of technology may expose the citizens to numerous rights abuses. In this work, the researchers made some key findings which include the deployment of some of these laws in a wrong manner and the need for amendments to some provisions of the law.

Keywords: Artificial intelligence, Emerging Technology, Data Protection, Cybercrime and Legal Framework

1.0 Introduction

Artificial Intelligence (A.I) and other emerging technologies are limitless in terms of the scope of its ability. Every passing day, scientist continually innovate new species of technological advancement, which both positively affect the legal jurisprudence or when improperly applied, translates to several legal violations.

The researchers by this work seeks to interrogate the various risks and benefits of Ai and other emerging technologies and appraise the country's legal frameworks with attention on not only the wordings of the law but how there are being interpreted and applied.

^{*} **Ifeanyi Maxwell Okobia**, Esq., Principal Partner, I.M. Okobia and Associates (Legal Practitioners & Arbitrators), Asaba, Delta State. Email: okobiaifeanyi@gmail.com; +2348130433738.

1.2 The Benefits of Technology

1.2.1. Technology as a Tool for Data Security

Data security in Nigeria is extensively provided for under section 39 of the Nigeria Data Protection Act, 2023. The NDPA requires the data controller or processor to implement technical means to ensure the security, integrity and confidentiality of personal data of Nigerians in their possession or under their control.¹ The Act further suggests some of the technical measures such as;

- a. Pseudonymization of personal data²
- b. Encryption of personal data³
- c. Regular updating and introduction of new technical measures to accommodate evolving risk⁴

The importance of technology in the protection and preservation of the rights of data subjects cannot be overemphasized. Encryption and pseudonymization of personal data are only possible with technologies.

Conversely, the absence of some technologies will entail difficulties in the effective management of personal data of data subjects in a manner that will ensure its security integrity and confidentiality.

1.2.2. Technology as a Tool for Effective Case Management and Quick Dispensation of Justice

Some notable innovations in the Nigeria legal justice adjudication aided by AI and other emerging technologies includes: audio visual court proceedings recording, e-filing of processes, electronic services of processes, virtual hearings of court proceedings amongst others.

The effective implementation of the above technologically advanced justice adjudication processes has the capacity to abridge duration of trial and time frame of adjudication by 50%.

These technological advancements eliminates completely adjournments taken because of the absence of either of the counsel, a witness or failure to reproduce inmates in the case of a criminal trial, as all parties can participate from wherever location he/she is across the globe; including filling and receiving service of court processes from such locations.

The tedious procedure of physically deposing to an affidavit or witness statement on oath before a Commissioner for Oath or producing hard copies of court processes and bringing them physically to be manually accessed and filed have been eliminated by the emergence of technology which has been ably aided by amendments to the Evidence Act, enactment of new laws and practice directions⁵.

Technology has ultimately made justice delivery less tedious, less time consuming and more efficient.

1.2.3. Technology as a Tool for Crime Detection, Investigation and Control.

Technology at the crime scene can be used to real-time capture information. Scenes relating to crimes such as burglary, car hit-and-run, assault, robberies, rape etc are easy for the police to

¹ NDPA, 2023, s.39(1).

² Ibid, s. 39(2) (a).

³ Ibid, s. 39(2)(b) NDPA currently applied by social media platforms

⁴ Ibid, s. 39(2) (g).

⁵ Section 109 of the Evidence Act 2011 (as amended), Part IV of the Delta State Administration of Civil Justice Law, 2022 and Practice Direction, Delta State, 2024.

conjure up with the aid of technology such as CCTV, DNA, fingerprints, glass and paint fragments, fibres, blood forensic examination etc.

Technology can also be used to predict and detect crime through technologically aided surveillance and monitoring, rapid identification systems and other software for biometrics, data retrievers and computer gadgets tracking. Drawing on advanced algorithms capable of forecasting criminal activity or predicting the strange movement of persons, information or patterns of behavior among persons; insights can be provided into where and how to deploy law enforcement officials to prevent the commission of crimes or easily identify where a crime is committed and the offenders.

Conclusively, the adoptions of forensic technologies have improved wholesomely, the quality of investigations; the reliability of evidence presented in court and reduced the probability of wrongful convictions. For example DNA evidences are essentially used in identifying perpetrators of violent crimes and other offences where the offender was not physically apprehended at the crime scene.

1.3 The Risks of Technology

1.3.1. Emergence of Cybercrimes

The term “cybercrime” was introduced after the latest evolution in the computer industry networks. Cybercrimes are considered a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of system and also, it can affect an organization’s reputation.⁶

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. Cyber criminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment⁷.

The emergences of technological advancements are with both benefits and risks. One of the risks is the big rise in the number of cybercrimes committed. It can be argued that there are not enough security measures and regulations to help protect these technologies as well as covering of tracks is much easier when committing a cybercrime than real crimes⁸ The most common types of cybercrimes are:

- a. Phishing and scam
- b. Identity theft
- c. Ransom ware attack
- d. Hacking
- e. Internet fraud
- f. Cyber bullying
- g. Cyber stalking
- h. Software piracy
- i. Social media fraud
- j. Online drug trafficking
- k. Electronic money laundry
- l. Cyber extortion
- m. Intellectual property infringements

⁶ Sherif Hasleir; what is cyber crime? Types, examples and prevention. <http://cybertalents.com> accessed 18/8/2023.

⁷ Ibid.

⁸ Ibid.

n. Online recruitment fraud.

Michael Aaron Dennis argued however that any other regular crime can be classified as a cybercrime as long as it is committed with the aid of computer and technology⁹ The FBI reports that while cybercrimes grow in prevalence and sophistication, so do associated costs for recovery and prevention¹⁰

1.3.2. Sophisticated Money Laundry

The crime of money laundry has become more prevalent with the emergence of technology. Money laundry refers to a fraud transaction scheme that aims to conceal the identities, source and destination of illicitly obtained money. Though traditional money laundry is synonymous with cash movements, the proliferation of technological developments including crypto currencies, technological banking has made money laundry also technologically sophisticated.

A money launderer can use digital currencies like Bitcoin to transfer money anonymously across border. Criminals may also use crypto wallets or peer-to-peer exchange to obscure the origin and ownership of illegal funds.

A combination of different technological advancements can relatively aid the commission of this crime of money laundry and/or make the tracing of this laundered money or the identity of the criminal very difficult or impossible.

1.3.3 Privacy Right breaches

AI privacy concerns are growing as artificial intelligence becomes more widespread, raising issues about how data is collected, used and protected. While AI can increase efficiency and improve work flow, it also introduces risks such as data security and illegal data use. Many individuals are deeply troubled about having their information harvested to train AI models without their consent.¹¹

The collection and use of personal data for AI has grown significantly. From social media interactions to smart gadgets, AI systems collect massive amounts of data to improve user experience, personalize content and drive targeted advertising. Clearly, this vast data collection poses substantial privacy risks.¹² It is submitted that in a scarcely regulated world of artificial intelligence, privacy/ data right breaches are almost impossible to prevent.

As it seems, the sky might be the limit for the level of AI sophistication, but as ubiquitous as AI has become, data privacy concerns are among the loudest concern of the public. It is indeed hard to argue with the benefits of a data-driven AI and other emerging technologies, but data collection and personal information processing can cause the following issues:

- a. Unauthorized access to personal information/data
- b. Re-identification from anonymized data sets
- c. Sensitive information/data disclosure

⁹ Michael Aaron Dennis, cybercrime; Definition and examples. <http://www.britannica.com> accessed 18/8/2025

¹⁰ Cyber crime, federal Bureau of Investigation, Economic Impact of Cyber Crime, Center for Strategic and International Studies.

¹¹ Kathryn Timonia; understanding AI privacy: key challenges and solution. <http://e.week.com/artificial-intelligence>. accessed 18/8/2025.

¹² Ibid.

d. Data profiling and unconsented data disclosures.¹³

Utilizing data-based AI innovations while protecting individual privacy will also be a genuine challenge. No matter the kind of legal framework that is put in place, AI technology tend to evolve much faster than the regulating frameworks.

It is noted that there are regulations that addresses data concerns that at least partially impact AI development and deployment, however some jurisdictions have gone ahead to make AI specific regulatory initiatives.¹⁴

2.0 Appraisal of Nigeria's Legal Frameworks

2.1. The Nigeria Data Protection Act, 2023

This law is currently Nigeria's most specific law/regulation on data rights protection of her citizens/ data subjects. The law tends to by its wordings and collective interpretation place data protection/information privacy as a specie of the fundamental right of privacy. Some courts agree wholly that data protection/informational privacy is indeed a fundamental right taking its root from Section 37 of the constitution which guarantees right to privacy,¹⁵ whereas some other courts and indeed some scholars in the field of data protection are not entirely convinced.¹⁶ The notable provisions of the Act are the rights accorded to data subjects and the responsibilities/obligations placed on data processors/controllers.

At this juncture, it is pertinent to ask a burning question. Where do AI and other emerging technologies fall into in the provisions of the NDPA? The answer to this will enable us conclude on the nature of control the Act has over the deployment/use of AI and other emerging technologies in connection to the informational privacy of Nigerians.

In answering this question, it becomes inevitable to reproduce and analyze the Act's definitions of the following:

1. Data subject
2. Processing
3. Data controller
4. Data Processor
5. automated decision-making
6. Data controller or data processor of major importance
7. Personal data

¹³ Krasimir Kuncher; Artificial Intelligence and privacy: Issues and challenges. [http://scale focus.com](http://scalefocus.com) accessed 15/8/2025.

¹⁴ For example, China's regulations on Algorithm, U.S National Institute of Standards and Technology (NIST) AI Risk Management Framework.

¹⁵ *Digital Rights Lawyers Initiative v NIMC (2021) LPELR-55623(CA), Incorporated Trustees Of Digital Right Lawyers Initiative v L.T. Solution & Multi Right Ltd.* unreported judgment of the High Court of Ogun State, Abeokuta Judicial Division, Coram Hon. Justice O.Ogunyowa, Delivered on the 9th day of November, 2020, Suit No:HCT/26/2020, See also the recent case of *Araka v E-Cart*, unreported judgment of the Federal High Court of Nigeria, Sitting in Abuja. Coram Hon. Justice Emeka Nwite, delivered on the 18th day of February, 2025 in Suit No: FHC/ABJ/CS/195/2024

¹⁶ *Incorporated Trustee of Digital Rights and law Initiative v Habab Ola Sunkanni Rajake*, unreported, Cited in *Solomon Okedera; Digital Rights in Nigeria: Through the Cases (CL Plus Ltd, 2022)*, *DRLI v Unity Bank Plc*, Unreported judgment of the FHC, Abeokuta Judicial Division Coram Hon. Justice Ibrahim Waltida, delivered on the 9th day of December, 2020 in suit No: FHC/AB/CS/85/2020

The Act in section 65 defines a data subject as: “an individual to whom personal data relates” This definition is vague especially as the word “individual” is loosely used here. Who qualifies as an individual here is uncertain and some scholars opined whether a corporate body will qualify as an individual.¹⁷ For the purposes of this discussion, it is also a right question to ask whether, a robot can also qualify as “an individual”. In the Act’s definition of data subject, the privacy professionals captured their collective displeasure to the “individual” used by the NDPA thus; ‘It is unclear whether the definition extends to both natural and artificial persons, the ambiguity and issues it might bring is further highlighted by the development of AI and Robotics and the recognition of robots as persons by some countries of the world.’¹⁸

Until a court’s decision on this, we will assume that the individual used in the NDPA only applies to natural persons. This is supported by the fact that other data protection legislation around the world used the term “natural persons” as against “individual” used in the NDPA¹⁹. It is also our submission that since some courts, scholars and indeed the NDPA sees data protection/informational privacy as a specie of the fundamental right of privacy guaranteed under Section 37 of the Nigeria’s constitution, it is absurd to argue that artificial persons, like a robot qualifies as a data subject thereby entitling them to or equating them to Nigerian citizens entitled to the enjoyment of the fundamental right of privacy. Indeed, the courts have held that only natural persons are entitled to enjoy the fundamental rights provisions of the constitution.²⁰

The term ‘processing’ was defined by the NDPA thus; “any operation or set of operation which is performed on personal data, whether or not by automated means such as collection, recording, organization, structures, storage, adaptation, alteration, restructure, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria”²¹

It is manifestly clear that the above activities which amount to processing are usually carried out by AI and other emerging technologies. I.M. Okobia posited thus;

“The activities that make up processing of personal data are numerous and it can be presumed that anybody or thing who does any of the above listed activities is a data processor, it is also my conclusion that anybody who defines the purpose and means any of the above listed activity is to be carried out is a data controller”²²

¹⁷ Olamide Babalola and others, implementing NDPA in the Nigeria way, from the professionals’ thoughts to the regulator’s Ears (Exclusive Privacy professional round table on the Nigeria Data Protection Act, 2023), held at the law office of Olamide Babalola in December 2023.

¹⁸ Ibid.

¹⁹ I.M Okobia and E.E. Ehigiator; An appraisal of the key forum of the NDPA 2023 Paul University, Awka, Faculty of Law Journal, Article 1 of the African Union Convention on Cyber Security and Personal Data Protection.

²⁰ *All Jaafariyya Development Association & Anor v Government of Kano State & ors* (2021) LPELR-57168(CA).

²¹ NDPA, 2023, s. 65.

²² Okobia, Ifeanyi Maxwell, *An Appraisal of the Nigeria Data Protection Act, 2023*, unpublished LLM Thesis submitted at Faculty of Law, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Campus.

From the collective interpretation of the above, it can be strongly argued that AI and emerging technologies are data processors and are used for data processing.

It is pertinent to note that the NDPA provides for rights of data subjects and obligations to data controllers only. The NDPA also anticipates that data processing and a data processor will require the input of a data controller.

This foundation to the mind of the researchers is faulty as the technologies already in use including robots do not need human assistance to function. There are already programmed to perform tasks based on data received.

What these technologies do without human intervention or input is what the NDPA term “automated decision making”²³ This automated decision making extends to profiling.

Generally, the NDPA outlaws this kind of activity. Specifically, it provides thus; ‘A data subject shall have the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject’²⁴

In analyzing a similar provision in the GDPR, the following comment was made;

“The GDPR introduced strict rules when it comes to processing of personal data that is done without human involvement. This encompasses different types of profiling, such as health, personal preferences, interest, reliability, behavior, or locations, if it produces a legal effect that significantly affects them”²⁵

The NDPA however, provides for some derogations and limitations to this right against automated decision making and profiling.²⁶ There are:

- a. Where the decision is necessary for entering into or the performance of a contract between the data subject and a data controller.
- b. Where the decision is authorized by a written law, which establishes suitable means to safeguard the fundamental rights and freedom and the interest of the data subject or
- c. Where the decision is authorized by the consent of the data subject.

Therefore, when it comes to Nigeria presently, the sky is not the limit for AI and other emerging technologies.

2.2. Cyber Crime (Prohibition, Prevention, ETC) (Amendment) Act, 2024.

The Act has laudable aims to combat online fraud and cyber-attacks.²⁷ However, as argued by Ambassador Richard Mills Jnr, rather than meeting the aims, the country has resulted in using the law to silent criticism and dissent.²⁸ He further argued that this approach has the potential of

²³ NDPA 2023, s. 65.

²⁴ Ibid, s. 37(1).

²⁵ What are the 8 Data Subject Rights According to the GDPR. //http Data privacy management.net Accessed 8/06/2024.

²⁶ NDPA 2023, s. 37(2)(a)(b)(c).

²⁷ Ambassador Richard M. Mills Jnr; preventing misuse of the Cyber crime Act: protecting free speech and Unlocking Economic Growth.http:www.n.g.usembassy.gov. accessed 17/8/2025.

²⁸ Ibid.

detering the innovation needed for economic growth.²⁹ In a further criticism of the Act and how it is applied, Ambassador Richard Mills Jnr argued thus;

“The cybercrime Act broad language, especially its vague definition of “false information”, “cyber stalking”, “harassment” and “insult” leave room for confusion and potential abuse. The law’s broad scope allows it to be misused against Nigerian citizens seeking to suppress dissent, form opinions or criticize powerful people”³⁰

This argument and opinion is well founded especially in the light of what has happened to persons like Dele Faratomi whose case the Ambassador referred to as a case study in support of his submissions. The law, though with laudable aims, has been misdirected and misapplied as a tool for political vendetta and oppression of dissenting voices and citizens by powerful people. The implications extend beyond free speech. Nigeria’s economic future depends on its ability to innovate and attract investments in the digital age of artificial intelligence and other emerging technologies.

Nigeria and indeed other countries across the world are grappling with the ever-evolving challenges and opportunities that the digital world presents, a properly drafted and implemented cybercrimes law is what is needed in age and times like this.

It is argued that the present Nigerian legislation on cybercrimes are not far from ideal, what is far from ideal is the manner of its misuse.³¹

At this juncture, we will proceed to analyze the provisions of the Act that has its implication on AI and other emerging technologies. Generally, beside the Section 24 of the Act usually applied maliciously against citizens, opposition, critics and journalists, the whole law is filled with noble provisions that criminalizes and punishes several cybercrimes.

As noted earlier, there are varying kinds of cybercrimes such as identity theft, cyber terrorism, computer related fraud and so on. In a bid to prevent and prohibit such crimes the Act in the following sections are noted with laudability. Sections 3 which designate certain computer systems or networks as critical national information infrastructure; Section 6 which provides for unlawful access to a computer, Section 8 which provide for system interference. Sections 9, 11, 12, 13, 14 and so on provides similarly for other cybercrimes.

What is notable here is that the offences are supposedly to be committed by an individual or corporation with the aid of computer and/or technology. If there is a way a computer, software or AI models can be pre- programmed to commit fraud or other crimes, can the law as it is be sufficient to attend to same?

²⁹ Ibid.

³⁰ Ibid.

³¹ Ben Ezeamalu; Nigeria cyber crime law still used to harass citizens despite amendment <http://www.the African report.com>. Accessed 17/8/2025. See also Festus Ogun Understanding Nigeria’s cyber crimes Act and its implementation mechanisms <http://www.the cijd.org> accessed 16/8/2025, Jonathan Rozen; Nigeria’s cyber crime reforms leaves Journalists at risk. <http://www.aljazeera.com> accessed 16/8/2025

For instance, a software or link created and an unsuspecting individual who tried to use the software for a useful purpose fall victim of a cybercrime. Or a system failure in an app or software occurs which exposes users to varying kinds of cybercrimes or loss of vital data or monies to individuals who then take advantage of the mishap.

Most Sections of the law commences with “A person who ...commits an offence”.³² A question that comes to mind is how accommodating is the term “a person who”. The researchers are also aware of the principles of vicarious liability and criminal responsibility of which the innovator of the software or application maybe held to be the offender especially when there is an intention to cause such crimes to be committed by the creation/programming of the software or application³³, it is however argued that the prevention and prosecution of these kind of offenses could be much easier if the law makes exacts provisions for them.

The Act interestingly in Section 23(1) provides thus; “A person who intentionally uses any computer system or network in or for.”³⁴

What is seen herein is that for one to be liable of an offence under this section, one must intentionally use any computer system or network in or for the commission of the crime. Now, does the criminal responsibility extend to one who creates or innovate a system/app/network or software that makes the commission of this crime possible but did not use it in person to commit the crime?

A great example is the creation of a VPN application which makes cyber criminals able to operate from a different location online while in another location offline. This makes the cybercrimes seamlessly committed and the criminals difficult to trace and apprehend. Now is there a possibility that the laws are wide enough in scope and reach to accommodate the creators of this system to be similarly guilty in the crimes committed with the aid of their innovations or digital creations?

The above leads us the provision of Section 28 of the Act. It provides thus;

- A person who unlawfully produces, supplies, adopt, manipulate or procures for use, imports, exports, distributes, offers for sale or otherwise makes available;
- a. any device, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act,
 - b. A computer password, access code or similar data by which the whole or any part of a computer system or network is capable of being accessed for the purpose of committing an offence under this Act or
 - c. any device, including a computer program designed to overcome security measures in any computer system or network with internet that the devices be utilized for the purpose of violating any provision of this Act, commits an offence ...

³² See Section 18, 21, 23 of the Act.

³³ See generally, Okonkwo and Naish: *Criminal Law In Nigeria* (Spectrum law series).

³⁴ The provision of child pornography and related offences.

Well, it seems the question of the liability of a creator of a system meant to be used for the commission of crime is provided for. However, the researchers wonder why the qualifier “unlawfully” was used in the Section. Does the Act anticipate a situation that someone can lawfully create a system meant to be used for the commission of crime? Or be licensed by the authorities of government to make such creations? We do not think so.

It is also observed in the Act that whatever crime the innovated system/app/software or network was used to commit, the innovator’s offence/punishment is not connected to it, except it results in loss or damage.³⁵ But what amounts to loss or damage or the weight of the loss or damage to qualify under this Section is left undefined by the Act. Its vagueness makes its application difficult and subject to abuse or multiple interpretations.

Conclusively, the Cyber Crimes (Prohibition, Prevention ETC) (Amendment) Act, 2024 is a noble legal framework to have in this digital age and time with only amendments demanded in the manner of its application and in some vague provisions.

2.3 Money Laundering (Prevention and Prohibition) Act 2022

Advancements in technology and AI can either aid in the crime of Money laundry or help in the effective prevention of the crime. The future of anti-money laundry lies in the continuous adaptation of emerging technologies. As criminals evolve their techniques, so must its methods of detection and prevention. It is pertinent to find out if the law on money laundry in Nigeria is able to accommodate new methods of detection and prevention.

Traditionally, money laundry usually involved cash and paper currencies. But with virtual assets, the crime of money laundry can no longer be limited to paper currencies especially in our laws.

AI and machine learning can analyze vast amount of data quickly and accurately. They can identify patterns and anomalies that might indicate money laundry. Emerging technologies are not without their challenges, thus, integrating new tools into existing anti-money laundry framework can be complex. However, the benefits of these technologies outweigh the difficulties.

It is on the strength of the foregoing that the new Money Laundry Act, 2022 is applauded by many stakeholders. The additions in the new Act may be few, but it at least provides a background upon which sophisticated and technologically enhanced money laundry can be tackled.

It is fascinating to note that some scholars are developing the trend of “cyber money laundering crime”.³⁶ In analyzing how it works, the learned author stated thus;

Before the emergence of mobile technology, clients made transactions at bank branches. The financial institution analyzed the legitimacy of the transaction received and was responsible for protecting and securing the resources. When using mobile applications, clients are responsible for protecting their access codes and passwords...Hackers and cyber criminals leverage this ignorance to

³⁵ Section 28(4) of the Act.

³⁶Jose-de-Jesus Rocha-Salazar; Money laundering in the Age of cybercrime and Emerging Technologies.<http://intechopen.com> accessed 15/08/2025.

steal information and resources through various technological means which they use to steal and launder money.³⁷

Another form of cyber money laundry in this age and time is money laundry through digital assets and platforms. On this, the learned author wrote;

Blockchain technology within the management of crypto currencies offers the anonymity necessary to obscure the illegal origin of resources. Thus criminals can exploit the crypto currency market to commit money laundry. They can use resources from illicit activities to purchase crypto currencies, hiding transaction information from national and international regulators. They can also commit illegal activity in the digital environment, such as stealing crypto currencies and making online exchanges to launder the resources.³⁸

Let's now proceed to analyze the new Money Laundry Act 2022 to see if “cyber money laundry crime” is adequately provided for. Section 13 of the Act makes provision for new products, business practice and technologies. However, this Section is not encompassing enough. It only admits the possibility of new products and emerging technologies but leaves specific regulations thereof to “the regulating authorities”³⁹

Who are these regulatory authorities? The Act did not elaborate further who is or who are the regulatory authority(ies). In the definition Section of the Act,⁴⁰ what was defined is the term ‘regulator’ and it was defined thus; “Means competent regulatory authorities responsible for ensuring compliance of financial institutions and designated non-financial businesses and professions with requirements to combat money laundry and terrorist financing.”

Whoever this regulator or regulatory authority(ies) may be, we look forward to a very robust regulation on this.

Section 7(8) of the Act provides for the ‘blocking’ of accounts upon an order obtained from the Federal High Court when the possible origin of funds cannot be ascertained. ‘Funds’ is defined in the Act to include virtual assets.⁴¹ The Act went further to define virtual assets thus; “Means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes but does not include digital representations of fiat currencies, securities and other final assets”⁴²

From a community reading of the above highlighted provisions, what can be ascertained is that a more robust regulation on combating “cyber money laundry crime” is left to the regulatory authority(ies), however, when a financial institution or a designated non-financial business and profession observes a suspicious movement of funds which includes digital assets, whose origin

³⁷ Ibid.

³⁸ Ibid. See also Dupui's D, Gleason K. M, ‘Money Laundering with Crypto currency: Open Doors and Regulatory Dialectic. *Journal of financial crime*. 2020 Vol. 8.

³⁹ Money Laundry (Prevention and Prohibition) Act, 2022, s. 13(1).

⁴⁰ Ibid, s. 30.

⁴¹ Ibid.

⁴² Ibid.

is not possible to ascertain, they ought to apply to the Federal High Court for such account, fund or securities to be blocked. The Act even criminalizes failure to comply with this obligation.⁴³

It is left to be seen how effective these provisions can be in the light of the ever evolving technological advancement and artificial intelligence deployments.

3.1 Comparative Insight of the EU AI Act and an argument for or against its adoption in Nigeria

There is no AI specific law in Nigeria. What are being applied to AI systems are existing laws and regulations related to data privacy, consumer protection and cyber security. The importance of a specific AI law or regulation is being considered in jurisdictions across the world with different countries and region taking various approaches. We shall proceed to consider a leading AI law in the world which is the E.U AI Act and consider the possibility of adopting a similar law/model in Nigeria.

The use of artificial intelligence in the EU is regulated by the AI Act, the world's first comprehensive AI law. In April 2021, the European commission proposed the first EU artificial intelligence law, establishing a risk-based AI classification system. Like the EU's General Data Protection Regulation,⁴⁴ the EU AI Act could become a global standard.

The EU AI Act provides for the classification of AI system. AI Systems that can be used in different applications are analyzed and classified according to the risk they pose to users. The different risk levels mean more or less AI compliance requirements⁴⁵

The Act assigns applications of AI to three risk categories. First, applications and system that creates an unacceptable risk. Second, high risk application, lastly applications not explicitly banned or listed as high-risk are largely left unregulated.⁴⁶

However, some views of the Act opine that the AI Act defines four levels of risk for AI system to with; unacceptable risk, high risk, limited risk and minimal risk.⁴⁷

We shall consider the EU AI Act on this broader four risk levels.

a. Unacceptable Risk

All AI systems considered a clear threat to the safety livelihood and rights of people are banned. The Act prohibits eight practices namely:

1. Harmful AI-based manipulation and deception.
2. Harmful AI-based exploitation of vulnerability
3. Social Scoring⁴⁸
4. Individual criminal offence risk assessment or prediction

⁴³ Ibid, s. 7(10).

⁴⁴ GDPR

⁴⁵ European/europa.eu accessed 15/08/2025

⁴⁶ Jarrod Sadulski; Artificial Intelligence in Crime Detection: How Useful *Information Technology Blog/ American Military University*

⁴⁷ AI Act/shaping Europe's digital. <http://www.gidital-strategy.eu.europe.eu> accessed 13/08/2025.

⁴⁸ Such as government-run social scory of the type and in China. See <http://artificial intelligence act.eu> accessed 15/08/2025

5. Untargeted scraping of the internet or CCTV material to create or expand facial recognition data bases
6. Emotion recognition in work place and education institutions
7. Biometric categorization to reduce certain protected characteristics
8. Real-time remote biometric identification for law enforcement purpose in publicly accessible spaces.⁴⁹

b. High Risk

AI use that can pose serious risks to health, safety or fundamental rights are classified as high-risk. High-risk AI systems are subject to strict obligations before they can be put on the market.⁵⁰

c. Limited Risk

This refers to the risks associated with a need for transparency around the use of AI. The AI Act introduces specific disclosure obligations to ensure that humans are informed when necessary to ensure that humans are informed when necessary to preserve trust.

Also, providers of generative AI have to ensure that AI generated content should be clearly and visibly labeled, namely deep fakes and text published with the purpose to inform the public on matters of public interest.⁵¹

d. Minimal or No Risk

Generally, the Act did not introduce rules for AI that is deemed minimal or no risk. The vast majority of AI system currently used in the EU fall into this category. This includes applications such as AI enabled video games or spam filters.⁵²

Article 99 of the EU AI Act provides for penalties for the violation of any provision in the Act. Such penalties include fines. The Act also suggested member states of the EU to lay down her own rules on penalties and other enforcement measures, which may also include warnings and non-monitory measures. The Act provides that EU member states in laying down her own rules should take into account the interest of SMEs, including start-ups and their economic viability.

It is noted that the Act took it upon itself to specifically outline the punishment to be melted on violators to the prohibited AI practices referred to in Article 5. Article 100 of the Act also provides for administrative fines on union institutions, bodies, officers and agencies. A specific fine/figure was not provided for here, but suggest that when deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to some conditions.⁵³

⁴⁹ AI Act/Shaping European's digital filter .<http://digital.strategy.eu.europa.eu>. See also Art. 5 EU AI Act.

⁵⁰ Ibid See also Article 6, 8-18 of EU AI Act

⁵¹ Ibid

⁵² Ibid

⁵³ EU AI Act, Article 100(1) (a-g).

Another provision to note in the Act is that the Act recognizes other laws, which may remotely apply to AI and provides that the Act shall not affect the prohibitions that apply where an AI practice infringes those laws.⁵⁴

Other notable provisions of this Act includes Article 27 which provide for Fundamental Right Impact Assessment for High-Risk AI system and different obligations and responsibilities imposed on various persons with regards the deployment, use and creation of AI systems.⁵⁵

In Nigeria, there is no AI specific law as stated earlier. The absence of such a law can hinder the effective use of AI in the country or leave AI system in Nigeria generally unregulated. Leaving AI and other similar emerging technologies generally unregulated is not an advisable risk to be taken. The EU AI Act has set a standard that can be adopted by countries of the world including Nigeria. The classification of risks, imposition of penalties and measures in relation to the classes of risk is a model, which can be seamlessly adopted in Nigeria and applied subject to the unique culture and lifestyle of Nigerians. It is only advised that such law should be applied properly, so as not to turn it to a political tool to suppress technology oriented business enterprises or competitors.

4.1 Observations, Recommendations and Conclusion

Crimes have grown more sophisticated due to technological advancements. To combat this increased sophistication, law enforcement and law making must continue to evolve with technology. The Laws appraised herein will require a few amendments to cover loopholes highlighted as well as better approaches in terms of application and use of the Laws as against the politicizations of same.

It is also necessary the country begin to consider an AI specific Law or regulation. The European Union (EU), AI Act is a good foundation upon which the country's Lawmakers can build on, while taking into account our unique qualities as a nation.

⁵⁴ Ibid, Article 5(8).

⁵⁵ Ibid, Articles 16, 23, 24 and 26.