African Journal on Privacy & Data Protection

To cite: E Salami & I Nwankwo 'Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer' (2024) 1
African Journal on Privacy & Data Protection 220-247

Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer

*Emmanuel Salami**
Researcher, Faculty of Law, University of Lapland, Rovaniemi, Finland

*Iheanyi Nwankwo***
Research Associate, Institute for Legal Informatics, Leibniz Universität, Hannover, Germany

Abstract:

As with the rest of the world, artificial intelligence (AI) systems, including chatbots, medical AI systems, agricultural optimisation systems, and so forth, are witnessing increased deployment in Nigeria. AI presents novel opportunities for innovation and tackling inefficiencies in several sectors of the Nigerian economy. However, its proliferation may result in a plethora of concerns if not developed and deployed within the bounds of law and ethics. Such concerns include the compromise of human rights, reinforcement of unlawful discrimination, compression of the privacy sphere of individuals, violation of the right to data protection, and so forth. This article focuses on the threats and vulnerabilities inherent in the development and deployment of AI as it impacts the right to privacy and data protection in Nigeria. These concerns have necessitated AI regulations and policies across the globe, and there is a consensus that AI systems must ensure respect for human rights and the rule of law, generally, and the right to privacy and data protection, specifically. Given data's prominent role in the AI life cycle, it is not surprising that privacy and data protection laws provide a fertile

* LLB (Lagos), LLM (Hannover), PhD (Lapland); me@emmanuelsalami.com
** LLB (Nig), BL, PhD, CC; nwankwo@iri.uni-hannover.de

basis for assessing AI systems' compliance regimes. At the time of writing, Nigeria is drafting a national AI policy and has only recently passed a data protection legislation. However, Nigeria's AI regulatory strategy has not been adequately examined from the perspective of privacy and data protection law. Therefore, this article seeks to fill this gap by exploring the tension between data protection law and the AI data processing life cycle in the Nigerian context. First, it reviews Nigeria's AI strategy and existing data protection framework and argues that they might be inadequate to address the challenges posed by AI. The article then recommends measures for balancing privacy and AI innovations in Nigeria with global best practices. Finally, it concludes that a robust and principled approach to AI regulation is essential to safeguarding privacy and data protection rights in Nigeria.

Key words: artificial intelligence; data protection; privacy; Nigeria; AI policy

1 Introduction

Global discussions about artificial intelligence (AI) have gained momentum with recent advancements in generative pre-trained transformers (GPTs)' natural language processing.[1] Although AI systems have been deployed in several other sectors, including health care, banking and policing, the impressive output of AI chatbots continues to gain traction. Indeed, there have been success stories around AI systems: More efficient industrial operation management, production cost reduction, and timely solving of complex tasks are some examples.[2] There are also prospects that AI can help in realising global sustainable development goals,[3] and many other use cases keep evolving as AI matures in several fields.

However, AI systems are not infallible; they also pose some risks that some technology experts have acknowledged and even called for a pause in AI development until a set of protocols are agreed upon.[4] For instance, there is evidence of bias reflected in these systems, resulting in discrimination and other (related) human rights violations.[5] Given its capabilities, bad actors can use AI systems to increase surveillance, infringe on the right to privacy, or violate the

1 OpenAI 'GPT-4' 14 March 2023, https://openai.com/research/gpt-4 (accessed 30 March 2023); OpenAI 'Planning for AGI and beyond' 24 February 2023, https://openai.com/blog/planning-for-agi-and-beyond?utm_source=substack&utm_medium=email (accessed 30 March 2023). See also B Gates 'The age of AI has begun' 21 March 2023, https://www.gatesnotes.com/The-Age-of-AI-Has-Begun (accessed 30 March 2023).

2 J Jeong 'Introduction of the first AI impact assessment and future tasks: South Korea discussion' (2022) 11 *Laws* 73.

3 ITU 'United Nations activities on artificial intelligence (AI)' 2021, https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2021-PDF-E.pdf (accessed 30 March 2023).

4 See Future of Life Institute 'Pause giant AI experiments: An open letter', https://futureoflife.org/open-letter/pause-giant-ai-experiments/?utm_source=substack&utm_medium=email (accessed 5 April 2023).

5 FRA 'Bias algorithms – Artificial intelligence and discrimination' 2022, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf (accessed 23 March 2023).

rights of vulnerable or minority groups, among other socio-economic impacts.[6] Furthermore, AI development and deployment techniques can impact data protection and ethical principles such as transparency, data minimisation, purpose limitation, accountability, fairness, and so forth.[7]

These concerns are significant, and several regulatory approaches are being devised by international, regional and national authorities to tackle them. For example, the United Nations (UN) and some UN specialised agencies, such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO), have addressed AI-related issues from various perspectives, including human rights and ethics.[8] In his 2021 human rights report, the UN Human Rights Commissioner called for urgent action by states to safeguard human rights in the era of AI. According to him, '[t]he operation of AI systems can facilitate and deepen privacy intrusions and other interference with rights in a variety of ways'.[9] Similarly, the Organisation for Economic Cooperation and Development (OECD) adopted some recommendations on AI that include principles for responsible stewardship of trustworthy AI.[10]

In Europe, the European Union (EU) and the Council of Europe (CoE) have undertaken several initiatives and reforms covering various aspects of AI regulation. The EU, for example, has proposed an AI Act that adopts a risk-based approach to AI regulation.[11] An AI Liability Directive has also been proposed by the European Commission (EC), which aims to make it easier for victims injured by AI-related products or services to bring civil liability claims.[12] These proposals have been followed up with reform to the EU's product liability regime. This reform brings onto the radar emerging technologies, including AI. It will ensure that after product deployment, the factors for consideration when assessing whether a product is defective will include machine learning.[13] Furthermore, the EU High-Level Expert Group on Artificial Intelligence (AI HLEG) has

6 The Alan Turing Institute 'Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal prepared for the Council of Europe's ad hoc committee on artificial intelligence', https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688 (accessed 5 April 2023).

7 Jeong (n 2); FRA 'Getting the future right – Artificial intelligence and fundamental rights' 14 December 2020, https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights (accessed 23 March 2023).

8 UNESCO 'Recommendation on the ethics of artificial intelligence' 23 November 2021, https://unesdoc.unesco.org/ark:/48223/pf0000381137 (accessed 23 March 2023).

9 United Nations Human Rights Commission 'Right to privacy in the digital age' 1 October 2021 A/HRC/48/31.

10 OECD 'Recommendations of the Council on artificial intelligence' 22 May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 12 February 2023).

11 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts COM (2021) 206 final.

12 Proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM (2022) 496 final.

13 Proposal for a directive of the European Parliament and of the Council on liability for defective products COM (2022) 495 final.

published an Assessment List for Trustworthy Artificial Intelligence to help developers assess the trust level of their AI systems.[14]

The CoE, for its part, is working on AI issues that span several themes.[15] It has issued several recommendations, guidelines and reports, including a recommendation on the human rights impacts of algorithmic systems[16] and guidelines on AI and data protection.[17] In addition, the CoE is spearheading efforts to develop a convention on AI.[18] If this succeeds, it will be the first of such a treaty. It would establish certain fundamental principles, rules and rights to ensure that the design and deployment of AI systems respect human rights, the functioning of democracy and the observance of the rule of law.

In Africa, the African Union (AU) and some African sub-regional groups have started paying attention to AI.[19] For example, the African Union High-Level Panel on Emerging Technologies (APET) has held consultative expert meetings on AI and recommended developing a continental AI strategy for Africa.[20] As a follow-up, a draft of an AU-AI Continental Strategy for Africa is being finalised to be submitted to the AU member states for review and validation, after which a continentally-adopted version will be launched at the beginning of 2024 at the AU Africa Heads of State and Government summit.[21] Recently, the African Commission on Human and Peoples' Rights (African Commission) commenced a focal point study and expert consultation on the impact of AI, robotics and other new and emerging technologies on African human and peoples' rights.[22]

14 High-Level Expert Group on AI (AI HLEG) 'Assessment list for trustworthy artificial intelligence (ALTAI) for self-assessment' 17 July 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342 (accessed 12 February 2023).

15 Council of Europe's work in progress https://www.coe.int/en/web/artificial-intelligence/work-in-progress#01EN (accessed 28 March 2023).

16 Council of Europe 'Recommendation CM/Rec (2020) 1 of the Committee of Ministers to member states on the human rights impacts of algorithmic systems' 8 April 2020, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 (accessed 28 March 2023).

17 Council of Europe 'Guidelines on artificial intelligence and data protection' T-PD (2019) 01.

18 See Council of Europe 'Revised zero draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law' 6 January 2023, https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f (accessed 28 March 2023).

19 Diplo 'Artificial intelligence in Africa: Continental policies and initiatives', https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-continental-policies/ (accessed 5 August 2023).

20 AUDA-NEPAD 'The African Union artificial intelligence continental strategy for Africa' 30 May 2022, https://www.nepad.org/news/african-union-artificial-intelligence-continental-strategy-africa (accessed 5 April 2023).

21 AUDA-NEPAD 'Artificial intelligence is at the core of discussions in Rwanda as the AU high-level panel on emerging technologies convenes experts to draft the AU-AI continental strategy' 29 March 2023, https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging (accessed 5 April 2023).

22 African Commission 'Press Release: Inception workshop and experts' consultation on the study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa, 8-9 June 2023, Nairobi, Kenya', https://achpr.au.int/en/news/press-releases/2023-06-08/inception-workshop-and-experts-consultation-artificial-intelligence (accessed 8 August 2023).

Given the traction that AI has gathered globally, it is not surprising that several countries have begun addressing AI issues nationally through policies, regulations and strategies.[23] Thus, there seems to be a global consensus that AI must be regulated to ensure that while reaping the enormous benefits of such technology, it is not used to violate human rights or diminish societal values. Nigeria, like several other countries, is in the process of developing a national AI policy.[24] It has already set up a National Centre for Artificial Intelligence and Robotics (NCAIR),[25] and a National AI Volunteer Expert Group tasked with helping the government draft the national AI policy has concluded its work.[26] Furthermore, the National Information Technology Development Agency (NITDA) has begun drafting a Code of Practice for AI to regulate AI tools such as ChatGPT.[27] While Nigeria's efforts at regulating AI are still at an infant stage, there is an expectation that all these efforts will culminate into a holistic framework that will adequately address emerging AI issues.

One aspect of AI development that has attracted regulatory attention is its impact on the right to privacy and data protection of natural persons (data subjects) whose data is processed to train the AI system or who are impacted by AI-based decisions. Undoubtedly, data is the critical raw material for developing and deploying AI systems – data is the input in AI systems' training, testing and operational processes.[28] Where this data relates to an identified or identifiable natural person (directly or indirectly), the privacy of these data subjects becomes crucial. Not surprisingly, this forms a starting point for measuring the compliance of AI systems within most regulatory frameworks.

Although privacy and data protection concerns are present in other information systems and applications, the design and operation of AI systems have distinct aspects that heighten the risks. These include using algorithms to discover hidden patterns; the opacity of the data processing; the tendency to collect excessive data; data repurposing; and the use of new types of data.[29] When critically analysed, these attributes raise questions as to whether AI systems can comply with data protection principles during their life cycle and to what

23 OECD AI observatory database on national AI policies and strategies, https://oecd.ai/en/dashboards/overview (accessed 5 April 2023).

24 'Developing the national artificial intelligence policy in Nigeria' *Premium Times* 12 August 2022, https://www.premiumtimesng.com/opinion/548380-developing-the-national-artificial-intelligence-policy-in-nigeria-by-fom-gyem.html?tztc=1 (accessed 20 March 2023).

25 https://ncair.nitda.gov.ng/?page_id=2584 (accessed 20 March 2023).

26 C Izuogu 'The artificial intelligence policy I envision for Nigeria', https://www.techpolicy.com.ng/the-artificial-intelligence-policy-i-envision-for-nigeria/ (accessed 30 March 2023).

27 E Ojukwu 'NITDA drafting the Nigeria Code of Practice for artificial intelligence tools such as ChatGPT and others', https://www.tekedia.com/nitda-drafting-the-nigeria-code-of-practice-for-artificial-intelligence-tools-such-as-chatgpt-and-others/ (accessed 8 August 2023).

28 International Organisation for Standards ISO/IEC TR 24368:2022 information technology – artificial intelligence – overview of ethical and societal concerns, https://www.iso.org/standard/74296.html (accessed 5 April 2023).

29 ICO 'Big data, artificial intelligence, machine learning and data protection' (ver 2.2 September 2017) 9, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (accessed 12 March 2023).

extent they could be used to exacerbate privacy violations. These concerns are compelling, given the ability of AI systems to discover unknown patterns and capabilities in surveillance, including through advanced facial recognition systems and profiling, among others.[30]

Therefore, it is not unusual for regulatory instruments to provide data subjects affected by AI systems with the agency over their data and accord them rights where privacy infraction occurs. Recent developments, for instance, allow data subjects to request an explanation of automated processes and human intervention to mitigate the risk of using a wholly automated system to process data that can significantly affect the data subjects. This approach is exemplified in the EU's General Data Protection Regulation (GDPR), which accords data subjects the right to information and 'not to be subject to a decision based solely on automated processing, including profiling'.[31]

Given this direction of travel, it is pertinent to look at Nigeria's AI policy and regulatory framework, especially at how these address privacy and data protection concerns in the context of AI systems' development and deployment. This is essential because AI systems are increasingly being deployed in several sectors of the Nigerian economy, including the financial, agriculture, health and education sectors.[32] As such, it is crucial to investigate how ready Nigeria's privacy and data protection regime is to address any concerns that might arise from using AI.

It is well-known that Nigeria's constitutional guarantee of the right to privacy is not detailed and may not have contemplated the complexities of emerging technologies such as AI systems. Thus, there has been a need for a more specific regulatory framework that defines how informational privacy is to be enforced. It was only in 2019 that the Nigerian Data Protection Regulation (NDPR)[33] was issued to regulate personal data processing, incorporating data protection principles and giving certain rights to data subjects. As this article is being drafted, the Nigeria Data Protection Act 2023 (NDPA)[34] was signed into law and would operate alongside the NDPR.[35] Although many observers have heralded these developments, there has been little investigation into how these instruments regulate AI development and deployment in relation to data protection implications.

Therefore, this article explores how these instruments address concerns around personal data processing throughout the AI systems' life cycles – development

30 ISO/IEC TR 24368 (n 28).
31 General Data Protection Regulation of 2016 arts 12, 13, 14 & 22.
32 D Eke and others (eds) *Responsible AI in Africa: Challenges and opportunities* (2023); K Bala and others 'Artificial-intelligence-based models coupled with correspondence analysis visualisation on ART – Cases from Gombe State, Nigeria: A comparative study' (2023) 13 *Life* 715.
33 https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf (accessed 12 January 2023).
34 Nigeria Data Protection Act 37 of 2023 A719-758.
35 Nigeria Data Protection Act 37 of 2023 sec 64(2)(f).

and deployment. The aim is to provide a primer on the potential challenges and privacy threats associated with personal data processing during the design and operational phases of AI systems in Nigeria, as well as recommend ways to address the gaps. The article is structured as follows: Part 2 defines artificial intelligence; part 3 gives an overview of Nigeria's privacy and data protection regime; part 4 analyses Nigeria's AI policy; part 5 explores privacy and data protection concerns associated with developing and deploying AI systems in Nigeria; part 6 discusses some salient findings of the articles, while part 7 provides some recommendations and concludes the article.

2 Defining artificial intelligence

As in the case of several other technological concepts, adopting a universal definition of AI has been challenging, especially because various stakeholders approach the concept from different perspectives. Moreover, several technologies exhibit different aspects of human intelligence and perform in an automated manner that falls within the realm of AI technology. Therefore, it is not surprising that no single definition that captures an array of technologies that could be termed AI has been agreed upon.

Several definitions could be cited to show this diversity. For example, the OECD defines an AI system as

> a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (eg with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy.[36]

While this definition attempts to capture several elements of AI, it sacrifices brevity. To forestall this, other entities have adopted a shorter definition. The International Organisation for Standards (ISO), for instance, defines an AI system as 'an engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives'.[37] Academics have also contributed to the quest to define AI.[38] McCarthy, credited

36 OECD 'OECD AI principles overview', https://oecd.ai/en/ai-principles (accessed 28 February 2023). The revised draft of the proposed EU's AI Act also defines AI in similar terms as 'a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts' (n 11) art 3.

37 International Organisation for Standardisation 'ISO/IEC 22989:2022 information technology – artificial intelligence – artificial intelligence concepts and terminology', https://www.iso.org/standard/74296.html (accessed 5 April 2023).

38 Eke and others (n 32).

as the father of AI, defines AI as 'the science and engineering of making intelligent machines, especially intelligent computer programmes, related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable'.[39]

In Nigeria, a few attempts have been made to define AI at a policy level. For example, the NITDA's draft national data strategy defines AI as 'the creation of intelligent objects that work and react like humans to carry out certain tasks meant for intelligent beings without human intervention'.[40] This definition by NITDA is fascinating as it suggests that AI systems do not require human intervention, contrary to the reality of the technology in some cases.[41]

While the above definitions capture several elements of AI, they bolster the fact that stakeholders view AI from diverse perspectives, which makes it challenging to append a single meaning to the concept and calls for perhaps a practical approach to defining AI contextually, given the multifaceted nature and the several technologies (including robotics, automation and machine learning) around AI. This article does not focus on harmonising the various definitions. However, it suggests a contextual approach to the definition of AI to avoid overly complex conceptual definitions that create uncertainty and make it difficult for a lay person to understand. Thus, AI systems could be seen as intelligent systems designed to 'think' and 'act' like humans in various contexts, with varying levels of human intervention.[42] In this sense, AI can be contextualised by the specific task that the system is designed to perform.[43]

39 J McCarthy 'What is AI/AI basics', http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html (accessed 28 February 2023).

40 NITDA 'National data strategy draft' 2022, https://nitda.gov.ng/wp-content/uploads/2022/11/Final-Draft-National-Data-Strategy.pdf (accessed 30 March 2023).

41 There are many instances where AI systems require human input and intervention. See P Samuelson 'AI authorship?' (2020) 63 *Communications of the ACM* 22.

42 Using automated vehicles as a yardstick, the Society of Automobile Engineers classified six levels of human intervention required in automated vehicles. Level 0 comes with no automation at all; levels 1 and 2, the system takes over some of the driving tasks, but the driver is required to continually monitor the system and must take over the driving when necessary; level 3 requires less monitoring of the system by the driver; in level 4 the system is able to drive the car in normal operation and in defined surroundings while the driver can intervene at will; level 5 is the final and fully-automated and autonomous driving stage. See Society of Automobile Engineers 'SAE international releases updated visual chart for its 'levels of driving automation' standard for self-driving vehicles' 11 December 2018, https://www.sae.org/news/press-room/2018/12/sae-internationalreleases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-drivingvehicles (accessed 3 April 2023).

43 Based on their capability to function independently, AI systems can also be classified as Strong AI (also known as Artificial General Intelligence (AGI)) and Weak AI (also known as Narrow AI). Strong AI describes conscious, self-aware, self-teaching, independent and autonomous AI systems that can solve problems independently. Strong AI systems are largely futuristic and remain an academic discourse at the time of writing. On the other hand, weak AI systems focus on performing specific tasks with human intervention. See B Marr 'What is the difference between weak (narrow) and strong (general) artificial intelligence (AI)' 21 July 2021, https://bernardmarr.com/what-is-the-difference-between-weak-narrow-and-strong-general-artificial-intelligence-ai/ (accessed 28 March 2023); Society of Automobile Engineers (n 42). For further reading on the extent of human intervention required at the current level of human intervention, see Samuelson (n 41).

3 Overview of Nigeria's privacy and data protection regime

Nigeria is one of the countries with a constitutional right to privacy. Section 37 of the Constitution provides that '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. However, as Omotubora rightly noted, this provision only presents 'a general prohibition from interference';[44] the Constitution did not define privacy or give it a clear scope. The expectation, therefore, is that other laws will fill this gap, determining the boundaries of this right and the principles and conditions for any lawful interference with it. Over the years, several laws and subsidiary instruments have been advanced for this purpose. However, until recently, most of these are sector-specific or marginally contain provisions on privacy as incidental to their core objective.[45]

Recently, the Court of Appeal acknowledged that the contours of the right to privacy could be appreciated by looking at the various laws and regulations made in furtherance or limitation thereof and the judicial interpretation of their application in Nigeria.[46] Therefore, any inquiry into Nigeria's privacy law must consider the various instruments that have been advanced to enforce or limit it. Apart from the pronouncement by the Court of Appeal above, the judicial interpretation of this constitutional right has also significantly influenced the development. Where necessary, the courts have examined these other instruments and have notably favoured a broad interpretation of the right to privacy in Nigeria. In *MDPDT v Okonkwo*, for instance, the Supreme Court declared: 'The sum total of the rights of privacy and of freedom of thought, conscience or religion which an individual has, put in a nutshell, is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary.'[47] To this end, the Court of Appeal has also pronounced that personal data protection is integral to the right to privacy guaranteed under the Constitution.[48] However, the Court has so far not established principles for personal data protection. Therefore, reliance would be placed on the principles in the secondary laws.

Apart from the judicial influence in this area, several regulatory authorities in Nigeria are reflecting the global trend by adopting data protection requirements

44 A Omotubora 'The NITDA regulations on data protection: A peculiarly Nigerian approach?' 28 June 2019, https://mikedugeri.wordpress.com/2019/06/28/the-nitda-regulations-on-data-protection-a-peculiarly-nigerian-approach/ (accessed 12 February 2022).

45 I Nwankwo 'Information privacy in Nigeria' in A Makulilo (ed) *African data privacy laws* (2016); UV Obi 'Data privacy and data protection law in Nigeria' 14 April 2022, https://www.mondaq.com/nigeria/privacy-protection/1183140/data-privacy-and-data-protection-law-in-nigeria (accessed 12 January 2023).

46 *Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission* Appeal CA/IB/291/2020.

47 *MDPDT v Okonkwo* (2002) AHRLR 159 (NgSC 2001) para 73; *Nwali v EBSIEC* [2014] CA/E/510/2013.

48 *Incorporated Trustees of Digital Rights Lawyers Initiative* (n 46) 23.

in areas where personal data processing is significant, such as banking and telecommunications. These regulators have issued many guidelines and codes of practice that impact data protection within their sector.[49] In 2019 NITDA published a general regulation, the NDPR, as an instrument of general application. NDPR imitated the EU's GDPR in several respects: It contains principles of personal data processing, the obligations of data controllers and processors, accords certain rights to data subjects and muted a few enforcement mechanisms.

However, NDPR has several shortcomings and has been severely criticised,[50] including for its peculiar language and structure and lack of independent supervisory authority. Most importantly, whether NDPR implements section 37 of the Constitution is unclear. Moreover, the courts have refused to enforce its provisions through the fundamental rights enforcement mechanism,[51] suggesting that its legal basis lies in the NITDA Act rather than the Constitution. It is also notable that NITDA has published two other guidelines, namely, the Guidelines for the Management of Personal Data by Public Institutions in Nigeria[52] and the Nigeria Data Protection Regulation 2019: Implementation Framework,[53] which are meant to clarify the provisions of NDPR. Surprisingly, in some respects, these documents have introduced new requirements beyond what NDPR provides, thereby creating uncertainty about their relevance.[54]

Given the shortcomings of NDPR, the NDPA has been welcomed by all stakeholders with the expectation that its implementation will fill the gaps in the system.[55] The Act provides a legal framework for personal data protection and aims, among others, to safeguard the fundamental rights, freedoms and interests of data subjects, as guaranteed by the Constitution.[56] It contains data protection principles, obligations of data controllers and processors, rights of data subjects

49 See the Central Bank of Nigeria Circular to Banks and Non-Bank Financial Institutions Issuance of Consumer Protection Regulations (20 December 2019); CBN's Framework Consumer Protection for Banks and Other Financial Institutions Regulated by CBN (2016); NCC's Consumer Code of Practice Regulation (CCPR) 2007; NCC's Registration of Telephone Subscribers Regulation 2011.

50 Omotubora (n 44). See also A Omotubora 'How (not) to regulate data processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)' (2021) 2 *Global Privacy Law Review* 186-199.

51 *Incorporated Trustees of Digital Lawyers Initiative (on behalf of data subjects whose personal data were exposed by the Unity Bank Plc) v Unity Bank Plc* (unreported) Suit FCH/AB/CS/85/2020; *Incorporated Trustees of Digital Lawyers Initiative (on behalf of Daniel John) v National Identity Management Commission* (unreported) Suit FHC/AB/CS/79/2020.

52 NITDA 'Guidelines for the management of personal data by public institutions in Nigeria, 2020', https://ndpb.gov.ng/Files/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal11.pdf (accessed 14 January 2023).

53 NITDA 'Nigeria data protection regulation 2019: Implementation framework' March 2021, https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf (accessed 14 January 2023).

54 Surprisingly, though, in some respects, these documents have introduced new requirements beyond what the NDPR provides. This has resulted in ambiguity and has possibly made the Nigerian data protection framework incomprehensible to lay persons.

55 It is remarkable that there have been several attempts at passing a federal data protection act in Nigeria since 2005. See Nwankwo (n 45).

56 Nigeria Data Protection Act of 2023 sec 1.

and enforcement mechanisms. Notably, the NDPA established the Nigeria Data Protection Commission (NDPC) to oversee its enforcement. The Act did not repeal NDPR; both instruments will operate concurrently.

As further discussed, the data protection principles in these instruments will impact the AI life cycle. For example, the NDPA requires that the processing of personal data must be lawful, meaning that it must be based on any of the permissible grounds listed in the Act, including consent, contract performance, compliance with a legal obligation, for the vital interest of the data subject, public interest task or legitimate interest of the data controller, processor or third party. The processing must also comply with other principles, such as purpose limitation, adequacy, data minimisation, storage limitation, accuracy, data security and duty of care.[57] In the same vein, AI systems must be designed to enable data subjects to enforce their rights, such as rights to information, rectification, erasure, not to be subject to a decision based solely on automated processing of personal data, among others.

In the following analysis, the relevant provisions of the NDPA and NDPR will form the focus of this article to determine their adequacy in regulating the privacy aspects of AI.

4 Artificial intelligence policy in Nigeria

As earlier noted, several AI systems are in use in Nigeria. These AI systems are used by various Nigerian institutions, including banks that deploy AI for anti-money laundering and credit risk assessment systems to ministries, departments and government agencies that use them for multiple services, such as deploying the vehicle identification number (VIN) valuation system by the Nigerian Customs Service.[58] Some of these AI systems are highlighted in Table 1 below:

57 Nigeria Data Protection Act of 2023 sec 24

58 D Olawuni 'Nigerian customs introduce new valuation system for imported vehicles' 14 January 2022, https://dailytrend.com.ng/2022/01/14/nigerian-customs-introduce-new-valuation-system-for-imported-vehicles/ (accessed 20 March 2023).

AI system/AI manufacturer	Function
Renewable Africa 365	This AI system has been developed to identify locations in Nigeria where solar power would be most viable and likely to impact the community positively.[59]
Thetaray[60]	Some Nigerian banks have deployed this AI system to identify suspicious transaction patterns that require further examination.[61]
Airsmat	Airsmat's AI system helps farm owners access information such as suitable crops to farm based on soil composition, crop count on the farm, weed and disease detection, etc.[62]
Ubenwa	This AI system supports the early identification of neurological and respiratory conditions in infants.[63]
Zenvus Smartfarm	This AI-powered precision farming solution uses an intelligent electronic sensor to help farmers optimise crop yields and reduce wastage by analysing soil data and providing real-time crop monitoring.[64]
Kudi.ai	Using natural language commands, this AI-powered chatbot allows users to perform various financial transactions such as bill payments, airtime recharge, and money transfers.[65]

Table 1: Some examples of AI systems in Nigeria[66]

Given the use of AI systems enumerated above and others not mentioned, it is not surprising that AI-related concerns have attracted regulatory attention in Nigeria, including that of NITDA, the government agency that promotes and regulates technology. In the Nigerian government's National Digital Economy Policy and Strategy, AI and machine learning are recognised as emerging technologies that will help boost Nigeria's economy and citizens' well-being and address national challenges.[67] Accordingly, NITDA has spearheaded the

59 'Harnessing AI for renewable energy access in Africa' 27 April 2021, https://ai4good.org/blog/harnessing-ai-for-renewable-energy-access-in-africa/ (accessed 21 March 2023).
60 https://www.thetaray.com/anti-money-laundering/ (accessed 20 March 2023).
61 A Pugh 'Nigerian fintech Arca taps ThetaRay for AI-powered AML solution' 8 September 2023, https://www.fintechfutures.com/2022/09/nigerian-fintech-arca-taps-thetaray-for-ai-powered-aml-solution/ (accessed 23 March 2023).
62 https://airsmat.com/farmmanager (accessed 23 March 2023).
63 https://www.ubenwa.ai/ (accessed 20 March 2023).
64 https://www.zenvus.com/products/smartfarm/ (accessed 20 March 2023).
65 https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria/ (accessed 20 March 2023). See also https://nomba.com/ (accessed 20 March 2023).
66 A perusal of the websites and relevant policies of these AI systems (and their developers) does not expressly reveal the types of data processed by these AI systems.
67 Federal Ministry of Communications and Digital Economy 'Nigerian government's national digital economy policy and strategy 2020-2030' November 2019, https://ndpb.gov.ng/Files/Policy-National_Digital_Economy_Policy_and_Strategy.pdf (accessed 20 March 2023).

establishment of NCAIR[68] and is developing an AI policy for Nigeria.[69] NITDA also established a National AI Volunteer Expert Group tasked with helping draft the national AI policy, which has completed its task.[70] At the time of writing this article, a draft of the AI policy has gone through NITDA's internal review and sent to the Federal Executive Council for approval.[71] Furthermore, NITDA has indicated it is drafting a Code of Practice for AI to regulate the use of AI tools, such as generative AI tools and their impact on privacy, bias, misinformation, deepfake, among other issues.[72] Amidst the risks associated with Large Language Models (LLM) like ChatGPT, NITDA intends that such a code will reflect the peculiar nature of the Nigerian environment to ensure responsible and ethical deployment of AI tools.

While this is ongoing, the Federal Ministry of Communications, Innovations and Digital Economy has hinted at its strategy on AI for Nigeria.[73] A White paper published by the ministry acknowledged that AI has evolved into a multifaceted technology with enormous economic and social potential. As such, the government is poised to adopt a 'co-creation' approach in developing Nigeria's AI strategy for sustainable development, with input from top Al researchers of Nigerian descent globally. The ministry has already started curating a list of leading researchers, in the hope that it will help build innovative technological solutions to solve national problems and create opportunities for citizens.

As of the time of writing, none of these initiatives has resulted in a concrete documented framework allowing a detailed analysis of privacy and data protection aspects around Nigeria's AI policy. In general, stakeholders have advised the regulator to adopt a rights-based approach in developing the AI policy, hoping this will eventually result in thoughtful laws and regulations that mandate responsible and trustworthy AI development and deployment.[74] The themes proposed for the futuristic policy include transparency, human rights, ethics, privacy and data protection, trust and robustness. These are laudable themes, and it is hoped that they will be at the forefront of any future policy to enhance AI advancement in Nigeria. In addition, they will assist in promoting competitiveness and societal respect for human rights and development. Therefore, policy makers must thoroughly evaluate the Nigerian environment,

68 https://ncair.nitda.gov.ng/?page_id=2584 (accessed 20 March 2023).
69 *Premium Times* (n 24).
70 Izuogu (n 26).
71 N Isaac 'FG finalises policy on AI, commends volunteers for contributions' 8 March 2023, https://sciencenigeria.com/fg-finalises-policy-on-ai-commends-volunteers-for-contributions/ (accessed 30 March 2023). Unfortunately, the draft was not publicly available for review at the time of writing in March 2023.
72 Ojukwu (n 27).
73 B Tijani, https://twitter.com/bosuntijani/status/1696113557354549599 (accessed 10 September 2023).
74 J Effoduh 'Towards a rights-respecting artificial intelligence policy for Nigeria' November 2021, https://paradigmhq.org/wp-content/uploads/2021/11/Towards-A-Rights-Respecting-Artificial-Intelligence-Policy-for-Nigeria.pdf?ref=benjamindada-com-modern-tech-media-in-ssa (accessed 30 March 2023).

including existing laws, and provide AI policies to enhance regulatory certainty and guide stakeholders in developing and deploying responsible AI.

5 Privacy and data protection concerns associated with AI systems in Nigeria

As established in the preceding part, the deployment rate of AI systems in Nigeria necessitates legal regulation. This part, therefore, will focus on the privacy and data protection regulatory aspects of AI in Nigeria and primarily considers AI systems in their development and deployment stages. AI's development and deployment stages are coinages of this article that underline critical stages in the AI life cycle. As will be discussed, some of the concerns and implications of AI systems arise in the machine-learning phase well before its launch. Some other concerns and implications arise after deploying the AI system and might be (un)connected to the machine-learning phase. The essence of this classification is to prevent convolution by approaching these privacy and data protection law concerns based on how they might occur. However, it is notable that some unavoidable overlaps may occur in such classification, especially concerning incidental and interrelated matters.

5.1 AI development stage

This is the phase where AI systems are created, potentially from the ideation stage to the actual building, testing and preparation of the AI for deployment. Undoubtedly, data plays an essential role in this phase.[75] Much of the progress achieved lately in AI development stems from the availability of more data for use in the machine-learning phase.[76] However, this stage is critical to AI's output because, with AI systems, the 'garbage in, garbage out' mantra holds ever true. Therefore, the output generated by the AI system is determined by the quality of the training data. To appreciate the criticality of data processing during the development phase and the tensions that may arise from a data protection perspective, some relevant issues will be considered in the context of the NDPR and the NDPA. Although these concerns are multifaceted and complex, the following analysis will primarily revolve around considerations, which include the legal basis for data collection, data quality and data minimisation.

75 J McKendrick 'The data paradox: Artificial intelligence needs data; data needs AI' 7 June 2021, https://www.forbes.com/sites/joemckendrick/2021/06/27/the-data-paradox-artificial-intelligence-needs-data-data-needs-ai/ (accessed 27 March 2023).

76 C Gröger 'There is no AI without data' (2021) 64 *Communications of the ACM* 98.

5.1.1 Legal basis for data collection

Data collection is a foundational phase in the AI development stage. Given its impact on AI's future deployment and output, this phase is critical because once the training or foundational data ingested by AI is tainted, that taint will likely reflect in and/or affect the data output. Where there is no reliance on a legal basis or a defective legal basis is relied upon to collect data for model training, the unlawful nature of the processing activity taints the data. This is particularly relevant when personal data is included in the large volumes of big data used to train AI systems. For instance, as of 2020, AI developer Clearview AI is said to have used about 4 billion pictures to train its facial recognition technology.[77] However, various data protection authorities have since fined Clearview AI for violating data protection principles, including unlawful data collection.[78]

The crux of this issue is that (global) data protection legislation, including the NDPA, requires that any processing of personal data shall be lawful, that is, rely on a legal base while complying with other applicable data processing principles and requirements. Irrespective of whether data used in training an AI model is obtained from open sources, failure to observe these legal requirements infringes the affected data subjects' rights. This is even crucial when data collection techniques, such as web scraping,[79] are analysed within the scope of data protection law.

A perusal of the website (including privacy policies/terms and conditions) of the AI developers/service providers listed in Table 1 does not mention or reveal how their data was collected for model training. However, there is no doubt that large volumes of (personal) data are required and must have been used to train these AI systems, thereby bringing this process within the purview of data protection law and necessitating compliance by all stakeholders. As such, any unlawful data processing at this phase embodies a risk that will likely affect the operational phase of the system and its output. One such risk is a possible suspension of the use of the AI system by supervisory authorities pending clarification of its compliance status, as seen with the Italian data protection authority's suspension of Open AI's ChatGPT and Replika in Italy.[80]

77 T Cushing 'How much data does clearview AI gather on people? The answer (sadly) will not surprise you' 27 March 2020, https://www.techdirt.com/2020/03/27/how-much-data-does-clearview-gather-people-answer-sadly-will-not-surprise-you/ (accessed 27 March 2023).

78 The French, Greek and Italian data protection authorities have variously fined Clearview AI for reasons related to unlawful data collection. See B Toulas 'Clearview gets third €20 million fine for illegal data collection' 21 October 2022, https://www.bleepingcomputer.com/news/security/clearview-ai-gets-third-20-million-fine-for-illegal-data-collection/ (accessed 27 March 2023).

79 Data scraping generally involves the automated extraction of data from the web. See Joint statement on data scraping and the protection of privacy, https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf (accessed 27 March 2023).

80 Garante per la protezione dei dati Personali 'Artificial intelligence: Stop to ChatGPT by the Italian SA personal data is collected unlawfully, no age verification system is in place for

An appropriate legal basis for data collection is a critical data protection consideration in all stages of the AI life cycle. NDPR provides, among other things, that personal data shall be lawfully processed based on consent, the performance of a contract, compliance with a legal obligation, the vital interest of the data subject, and public interest.[81] Section 25 of NDPA equally tows this line but includes an additional basis – 'legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed'. Suffice it to say that the Nigerian data protection framework covers personal data collection during AI development, irrespective of whether the data is obtained from open or closed sources.

On the part of the developers of the AI system, concerns around the issue of a legal basis for data collection can arise in two ways: first, when personal data that has not been lawfully collected (for instance, through web scraping devoid of an appropriate and justifiable legal basis) is used during the machine learning process.[82] This would result in unlawful data processing since the system has been developed with unlawfully-obtained data. Assuming that the AI systems identified in Table 1 above have been developed with data collected from Nigeria(ns), it is unclear what legal basis the developers would have relied upon to collect the data, as no evidence of this is publicly available on their website. Second, it is possible for AI systems to process (personal) data in a manner that was not intended at the commencement of the processing activity.[83] In such an event, the initial legal basis for the activity might not suffice again, particularly when considering that the data processing purpose has changed.[84]

5.1.2 Data quality

Another critical concern at the AI development stage is the quality of data used during machine learning. Again, where personal data is involved, the data protection principle of data quality requires that data controllers/processors process data that is accurate and fit for purpose. Therefore, using biased and/or inaccurate data that does not represent the targeted population, whether imported from offline sources or online, to train AI systems violates this principle. For example, biased data that contains the stereotypes existing in offline spaces, when imported into the AI system, can potentially result in the adoption of

children' 31 March 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english (accessed 2 April 2023).

81 Nigeria Data Protection Regulation of 2019 secs 2.1 & 2.2. See also Nigeria Data Protection Act of 2023 sec 25 for a similar provision.

82 The French data protection supervisory authority, CNIL, issued a fine against Clearview AI for similar reasons. See CNIL 'Facial recognition: 20 million euros penalty against clearview AI', https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai (accessed 27 March 2023). For further reading on web scraping, see B Sobel 'A new common law of web scraping' (2020) 25 *Lewis & Clark Law Review*, https://law.lclark.edu/live/files/31605-7-sobel-article-251pdf (accessed 27 March 2023).

83 D Bloch 'Machine learning: models and algorithms' 27 May 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3307566 (accessed 27 March 2023).

84 Nigeria Data Protection Regulation 2019 sec 2.1 (1)(a) for further grounds of data processing.

unlawful discriminatory practices by AI systems. A practical manifestation of this possibility has been observed in the United States, where the use of AI for (predictive) policing, including crime prediction, neighbourhood surveillance, vehicle plate number identification, facial recognition, and so forth, is fraught with discrimination imported from data sources with which the AI was trained.[85] During machine learning, a backlog of biased data is typically fed into the AI system, thereby systematically creating a bias in its outcome.[86] More specifically, reliance on racially-imbalanced data that reflects the racial sentiments of a human police officer will only train the AI to act like any other racially-biased human police officer.[87] Based on this use case, one can conclude that the importation of biased or inaccurate data at the data collection stage of AI can result in biased and other adverse outcomes.

As such, an argument can be made for a breach of the principle of data quality in these cases. The data quality principle can be gleaned from NDPR and NDPA through the data accuracy principle. NDPR provides that personal data shall be 'adequate, accurate and without prejudice to the dignity of the human person.'[88] NDPA is more detailed and provides that personal data shall be 'accurate, complete, not misleading and, where necessary, kept up to date regarding the purposes for which the personal data was collected or is further processed.'[89] Arguably, this provision seeks to guarantee data quality and adequacy throughout the life cycle of the processing operation. It even covers further processing (referred to in this article as data repurposing). Thus, AI systems developed in Nigeria with poor quality and biased data will potentially infringe on the law. Therefore, it is necessary that AI developers thoroughly check the quality of the data they use in training their models to be compliant with the relevant data protection law in Nigeria.

5.1.3 Data minimisation

The possible collection of more data than is necessary for the processing activity is another concern that is likely in the use of AI. According to the data minimisation principle, data controllers and processors are limited to collecting and processing only the minimum amount of personal data necessary to fulfil a specific purpose. NDPR reflects this principle in its requirement that personal data processed shall be 'adequate, accurate and without prejudice to the dignity of the human person'.[90] However, a more robust provision of the data minimisation principle has been included in NDPA, which provides that a data controller or data

85 AG Ferguson *The rise of big data policing: Surveillance, race, and the future of law enforcement* (2017) 93.
86 As above.
87 As above.
88 See Nigeria Data Protection Regulation of 2019 sec 2.1(1)(b).
89 Nigeria Data Protection Act of 2023 sec 24(1)(e).
90 Nigeria Data Protection Regulation of 2019 sec 2.1(1)(b).

processor shall ensure that personal data is 'adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed'.[91]

Traditionally, large volumes of data are required to train AI systems, including LLM, such as ChatGPT. For example, GPT-3 is reported to have 175 billion parameters and was trained on 570 gigabytes of text.[92] A related concern of excessive data collection is when AI systems capture data independently, especially those that use cameras to scan the environment or automatic speech recognition (ASR)[93] and speech-to-text software. There is the possibility to capture more data than necessary because, in most cases, these data-capturing Internet of Things (IoT) attached to AI systems will capture various data categories in the environment, whether needed or not. These examples run contrary to the data minimisation principle highlighted above.

In sum, while the concerns discussed in this part are not an exhaustive representation of the concerns associated with data protection during AI system development, they have been highlighted to show the tension between standard practices in AI development and relevant data protection principles in Nigeria. More importantly, these concerns may still be prevalent or overlap with others discussed next within the deployment context.

5.2 AI deployment stage

The deployment phase in the AI life cycle is when AI products and services are launched subject to their practical use cases. This phase is not devoid of possible data protection concerns. In the absence of proper planning and preparation, the potential consequences of the AI deployment stage can come as a surprise to AI developers and data controllers/processors. Although several concerns can arise at this stage, the following discussion focuses on transparency, data security, purpose limitation and automated decision issues.

5.2.1 Transparency

Although highlighted here, transparency requirements cut across both the development and deployment phases of the AI life cycle. For example, during data collection, the transparency principle requires providing data subjects with

91 Nigeria Data Protection Act of 2023 sec 25(1)(c).

92 A Tamkin & D Ganguli 'How large language models will transform science, society, and AI' 5 February 2021, https://hai.stanford.edu/news/how-large-language-models-will-transform-science-society-and-ai (accessed 27 March 2023).

93 ASR breaks down speech (either live or recorded) into segments, which are then analysed by the algorithm using natural language processing. For further reading, see D Yu & L Deng *Automatic speech recognition: A deep learning approach* (2014) 1-7.

information about the life cycle of the data processing activity.[94] The AI data deployment stage can also be fraught with transparency concerns. For example, AI systems can be developed with a level of complexity that might make it challenging to explain its functionality. This 'black-box' design means that AI systems may lack the transparency required for data subjects to understand how their data is processed, and decisions arrived at using the system.

In addition, the 'expectation of privacy' principle, handed down by the European Court of Human Rights (ECHR) and now a critical part of privacy law jurisprudence, can also be impacted by the transparency principle.[95] Without transparent information, data subjects will be deprived of their right to be aware of and anticipate the consequences of relevant data processing activities concerning them.[96] This can result in the erosion of trust and the limiting of accountability.

NDPR does not have a unique transparency principle. Rather, it subsumes this principle under the data subject's right to be provided with 'any information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language.'[97] NDPR further provides that data subjects are to be provided with transparent information before the commencement of the processing activity.[98] A more detailed provision is reflected in NDPA. Section 24(1)(a) of NDPA contains the fairness, lawfulness and transparency principles. The transparency principle requires that relevant information relating to the data processing should be clearly communicated to the data subjects. This principle generally applies to three central areas: providing information to data subjects related to the processing, including the risks and safeguards associated with the processing; how data controllers communicate with data subjects about their rights; and how they facilitate the exercise of these rights.[99]

To further bolster this principle, section 27 of NDPA lists the nature of the information to be provided to the data subject, including the 'existence

94 For further reading, see L Naudts and others 'Meaningful transparency through data rights: A multidimensional analysis' in E Kosta, R Leenes & I Kamara (eds) *Research handbook on EU data protection* (2021), https://ssrn.com/abstract=3949750 (accessed 2 April 2023).

95 This principle pertains to whether the data subject had reasonable expectations of privacy that justify or render an intrusion into their privacy (un)lawful. The origin of this principle is traceable to the jurisprudence of United States privacy law. See P Winn 'Katz and the origins of the "reasonable expectation of privacy" test' (2008) 40 *McGeorge Law Review*, https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1204&context=mlr (accessed 2 April 2023). The principle crept into European law around 1997 when it was applied by the ECHR in the *Halford* case. See T Gomez-Arostegui 'Defining private life under the European Convention on Human Rights by referring to reasonable expectations' (2005) 35 *California Western International Law Journal,* 2.

96 *Barbulescu v Romania* (12 January 2016) Application 61496/08. See also Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' 2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf paras 39-43 (accessed 2 April 2023).

97 Nigeria Data Protection Regulation of 2019 sec 3.1.

98 Nigeria Data Protection Regulation of 2019 sec 3.1(7); Nigeria Data Protection Act of 2023 sec 28.

99 See UN Right to Privacy Note by the Secretary-General (20 July 2022) A/77/196.

of automated decision-making, profiling, the significance and envisaged consequences of such processing for the data subject, and the right to object to, and challenge such processing'.[100] However, owing to its black-box design and the possibility of AI systems capturing data without the knowledge of the data subject, this may be problematic to achieve. An example of this can be found in AI systems that deploy sensors and cameras for data collection by capturing human faces.[101] In such cases, providing transparent information to data subjects might prove challenging because of the automated, spontaneous and large-scale nature of the data collection.

5.2.2 Data security

Multiple computer networking systems are necessary for AI to function correctly, necessitating considering the security of data being processed by these systems.[102] This is coupled with the large-scale multi-jurisdictional data transfers and IoT attached as components to some AI systems, all requiring varying levels of data security to protect (personal) data. The data security principle requires data controllers and processors to adopt technical and organisational measures to secure both data and systems used to process data to ensure confidentiality, integrity, and availability of personal data. AI systems can suffer glitches that raise significant data protection concerns without adequate security measures.[103]

Section 2.6 of NDPR provides, among other things, that anyone involved in data processing shall develop security measures to protect data, including protecting systems from hackers, setting up firewalls, access control, data encryption, and so forth. Similarly, NDPA includes a data security principle[104] and explicitly requires data controllers and processors to implement appropriate technical and organisational measures towards the security, integrity and confidentiality of personal data under their control.[105] Factors such as the amount and sensitivity of the personal data, the nature, degree and likelihood of harm to data subjects that could result from data breaches, the extent of the processing,

100 Nigeria Data Protection Act of 2023 sec 27(1)(g).
101 These data types are referred to as observed data that are recorded automatically, eg, CCTV cameras, cookies, etc. See Information Commissioner's Office (n 96) 12.
102 Note that data security issues can also arise during the development stage of AI, especially in relation to the processing of data for machine learning.
103 At the time of writing this article, it was reported that the famous AI system Chat GPT had suffered a security breach. See E Kovacs 'ChatGPT data breach confirmed as security firm warns of vulnerable component exploitation' 28 March 2023, https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/ (accessed 27 March 2023). For further readings on the vulnerabilities of AI and how they can result in security breaches, see M Comiter 'Attacking artificial intelligence: AI's security vulnerability and what policymakers can do about it' August 2019, https://www.belfercenter.org/publication/AttackingAI (accessed 27 March 2023).
104 Nigeria Data Protection Act sec 24(1)(f) and sec 24(2). See also sec 39.
105 Nigeria Data Protection Act sec 39.

data retention period, and so forth, must be considered by them in adopting appropriate data security measures.[106]

However, as stated earlier, maintaining an adequate security framework for AI systems can prove arduous because of the multiple parties and various IoT and data transfers, each susceptible to a vulnerability. Some possible causes of data breaches in AI systems include data tampering, model poisoning, insider threats, and so forth.[107] The criticality of data security to AI can be better appreciated when one considers the recent data breach recorded through Chat GPT and the volume of data affected in the process.[108]

5.2.3 Purpose limitation

A further concern at the AI deployment stage pertains to purpose limitation. The purpose limitation principle requires data controllers to only process personal data for a specified purpose. This is to forestall processing personal data as an afterthought and prohibit further processing, in general, unless such processing is compatible with the original purpose, subject to adequate safeguards and compliance with the relevant rules. In contrast, AI systems can, in some cases, generate results not anticipated at the beginning of the processing activity, and this can encourage data repurposing to achieve a new outcome. An example of this could arise when using unsupervised machine-learning techniques, which can potentially cause unanticipated data processing outcomes.[109] It is usually a suitable device for discovering underlying use cases for data. However, it can pose a concern to the purpose limitation principle.

The purpose limitation principle is reflected in NDPR in several ways. Section 2.5(c) of NDPR provides that the privacy policy shall contain the purpose of collecting personal data. NDPR further provides that should the controller intend to further process the personal data for a purpose other than that for which the personal data has been collected, the controller shall provide the data subject before that further processing with information on that other purpose, and with any other relevant additional information.[110] This provision captures the purpose limitation principle and the rules surrounding data repurposing.[111] Similarly,

106 As above. This provision of the NDPA has a stronger language than that of the NDPR, and quite comparable to the language of international legislation such as the General Data Protection Regulation of 2016 art 32.

107 E Nick 'Top 7 data security threats to AI and ML' 7 December 2022, https://www.datasciencecentral.com/category/business-topics/ (accessed 27 March 2023).

108 Kovacs (n 103). Employees have also inadvertently fed confidential information into AI systems. See L Maddisson 'Samsung workers made a major error by using chatGPT' 4 April 2023, https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgp (accessed 27 March 2023).

109 Unsupervised machine learning draws inference(s) from datasets without reference to known or labelled outcomes. See Bloch (n 83).

110 Nigeria Data Protection Regulation of 2019 sec 3.1(7).

111 See a variant provision on the rules of data repurposing in General Data Protection Regulation of 2016 Art 6(4). For further reading on data repurposing, see P Woodall 'The data repurposing

the purpose limitation principle is also captured in NDPA, which provides that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. Further processing is permissible for compatible purposes, such as scientific research, subject to appropriate safeguards, among other considerations.[112]

Therefore, should AI systems be used when their purposes cannot be identified at the beginning of the processing activity and/or maintained throughout the AI life cycle, this can infringe upon the purpose limitation principle. It is common practice to use (personal) data provided by AI users to train the said AI through machine learning.[113] This practice will negatively impact the purpose limitation principle, especially in the event of unsupervised learning.

5.2.4 Automated decisions

AI systems are used for automated decision making, impacting natural persons' rights and freedoms.[114] Using AI for automated decision making can result in unintended risks for data subjects,[115] including depriving patients of access to adequate medical treatment.[116] Given its criticality, it is typical for data protection legislation to include safeguards for the protection of the rights of data subjects. For instance, GDPR has accorded data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them.[117]

Although NDPR does not contain a similar right for data subjects, it provides, among other things, that in the use of automated decision-making tools, 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' shall be provided to them before data collection.[118] While this is encouraging, NDPA has filled the gap by providing the data subjects with a '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'.[119] Although there are exemptions to this right, the problem, as earlier identified, is that many AI

challenge: New pressures from data analytics' (2017) 8 *Journal of Data and Information Quality* 3-4.

112 Nigeria Data Protection Act of 2023 sec 24(4).

113 Eg, this is the practice with AI systems such as Chat GPT that use user data for machine learning. See Chat GPT FAQ, para 6, https://help.openai.com/en/articles/6783457-chatgpt-faq (accessed 4 April 2023).

114 This use case can be found when AI is used in making decisions pertaining to credit scoring, credit lending, mortgage applications, healthcare use, etc.

115 B Mittelstadt and others 'The ethics of algorithms: Mapping the debate' (2016) 3 *Big Data and Society* 2.

116 Z Obermeyer and others 'Dissecting racial bias in an algorithm used to manage the health of populations' (2019) 336 *Science* 447-453.

117 General Data Protection Regulation of 2016 art 22.

118 Nigeria Data Protection Regulation of 2019 sec 3.1(7)(l).

119 Nigeria Data Protection Act of 2023 sec 37.

systems have 'black boxes', making it difficult, if not impossible, to understand the logic behind their decisions. This poses a data protection compliance concern.

Notably, NDPA further requires data controllers to implement suitable measures to safeguard the data subject's fundamental rights, freedoms and interests, including the rights to obtain human intervention, express their views and contest automated decisions.[120] This is a welcomed development, considering that AI systems can be fraught with a large margin of error.[121] Such provision forces AI systems to be deployed in a manner that enables data subjects to enforce their rights.

6 Discussion

It can be observed from the preceding parts that Nigeria's AI policy is still being developed, offering little insight into how privacy and data protection concerns identified above could be tackled. It is uncertain at this stage whether the policy will result in a dedicated AI regulatory instrument such as the proposed EU AI Act that is being negotiated. Despite these shortcomings, there is evidence that NDPA and NDPR, key data protection instruments of general application in Nigeria, contain principles and provisions relevant to regulating AI systems' development and deployment. Although these instruments were not focused on AI when adopted, an analysis of their provisions indicates complementarity of how they can regulate data protection issues arising in the use of AI. For example, while NDPR contains neither the right not to be subject to a decision based solely on automated processing nor human intervention regarding such processing, NDPA has complemented this shortfall.[122] Similarly, the transparency principles that is missing in NDPR are now incorporated in NDPA.

One interesting distinction between NDPR and NDPA is that the former provides data subjects with a right to obtain 'meaningful information about the logic involved' in making automated decisions concerning them.[123] Such provision or its variant is absent from NDPA.[124] The right to explainability of automated decision making has undergone various stages of transformation from academic debates[125] to being featured in legislation[126] and pragmatic implementation. Therefore, it is necessary to retain this feature in the data protection framework to align with international standards in data protection law. Thus, the NDPC

120 Nigeria Data Protection Act of 2023 sec 37(3).
121 These errors could stem from various avenues including bias that originates from the developer's bias and the use of biased datasets.
122 Nigeria Data Protection Act of 2023 (n 119) .
123 See Nigeria Data Protection Regulation of 2019 art 3.1(7)(i).
124 See Nigeria Data Protection Act of 2023 sec 27(1)(g).
125 S Wachter and others 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2016) *International Data Privacy Law*, https://ssrn.com/abstract=2903469 (accessed 4 April 2023).
126 This provision is featured in the data protection legislations of some African countries. See, eg, South Africa's Protection of Personal Information Act (POPIA) 2013 sec 71(3)(b).

ought to take advantage of the complementarity of both instruments to avoid uncertainty.

Despite this complementarity, stakeholders should look beyond (the principles of) data protection law and take advantage of the global trend towards a holistic, ethical and risk-based approach to AI regulation. One of the benefits of the worldwide attention that AI has received is the enormity of work undertaken concerning AI regulation, which Nigeria can leverage. A notorious example is the report of the EU's AI HLEG, which can serve as a regulatory guide in shaping AI regulation in Nigeria.[127] One key output of the guidelines of the EU AI HLEG is that for AI to be trustworthy, it ought to be robust while complying with legal and ethical principles.[128] The EU's AI HLEG proposes seven key requirements to consider AI trustworthy. These seven key requirements are human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity; non-discrimination and fairness; societal and environmental well-being; and accountability.

Beyond the scope of data protection principles, Nigerian authorities could draw inspiration from global best practices in shaping Nigeria's AI policy direction. This will serve two essential purposes. First, it will ensure that AI systems manufactured in Nigeria are marketable to the rest of the world while ensuring privacy compliance that meets minimum global standards. Second, using international standards will help address the challenges identified in this article, particularly in using biased data during AI development. One possible way of tackling this concern is by adopting tools designed for detecting and mitigating bias in algorithms and ensuring that divergent data that pertains to a broad spectrum of people, cultures, issues, history, and so forth, is used to train AI systems deployed in Nigeria.[129] This way, data will represent various members and interests of society more, which will not be prejudiced by the traditional biases that society has become familiar with. Given Nigeria's lack of regulation, international best practices and ethics become essential to achieving this goal.[130] Therefore, it is suggested that stakeholders deploying AI systems must go beyond the letters of the law and consider ethical principles in the AI life cycle.

Similarly, more emphasis should be placed on using privacy-enhancing mechanisms, such as privacy impact assessments (PIAs) and privacy by design (PbD), especially in scenarios of large-scale data processing, such as web scraping,

127 AI HLEG (n 14).
128 As above.
129 Further measures such as process standardisation and AI/data auditing have been proposed to tackle the problem of biased data. See E Salami 'AI, big data and the protection of personal data in medical practice' (2019) 3 *European Pharmaceutical Law Review* 165-175. Furthermore, tools such as IBM's AI Fairness 360 help in examining bias in machine learning. See IBM 'Introducing AI fairness 360', https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/ (accessed 6 April 2023).
130 For further reading on ethical issues in big data processing, see M Kirsten 'Ethical issues in the big data industry' (2015) 14 *MIS Quarterly Executive* 2.

when developing AI systems in Nigeria. The PIA is a risk assessment tool to identify threats against personal data and other assets. It also analyses the threats and potential harms to the data subjects, aiming to implement measures to mitigate the risks.[131] It is 'anticipatory in nature' and ideally carried out before a project begins, before the risk occurs. On the other hand, PbD centres on embedding privacy consideration into the design specifications of technologies that process personal data or could affect privacy in general.[132] Both tools are proactively used for embedding privacy into the design and operation of personal data-processing activities.[133] These mechanisms are obtainable under Nigeria's existing data protection regime and could be critical to implementing the duty of care and accountability required under section 24(3) of NDPA.

The duty of care requirement provides that a data controller or processor owes a duty of care regarding data processing and shall demonstrate accountability with respect to the principles contained in NDPA. By so doing, NDPA creates a duty of care in favour of data subjects for processing their personal data by controllers and processors. The duty of care is a new introduction to the jurisprudence of Nigerian data protection law, though not entirely new to data protection law itself.[134] Scholars have also argued that a connection exists between the duty of care under the law of torts and privacy.[135] The notorious case of *Donoghue v Stevenson* lays the foundation for the duty of care principle, which requires that a person exercises a duty of care to foreseeable persons (the plaintiff) to prevent them from being harmed.[136]

On the other hand, the accountability principle requires that data controllers and processors should be able to demonstrate compliance with the principles of data protection law. While NDPA refers to the duty of care on only one occasion, it references the accountability principle on three occasions, signalling its importance. By adopting PIA and PbD, some of the concerns highlighted in part 5 of this article will be promptly identified in context, and mitigation will be planned early enough before or during the development of the AI system and/or launching it. Among other things, these mechanisms will ensure that data collection processes involve sufficient considerations of privacy compliance and

131 See I Nwankwo 'Towards a transparent and systematic approach to conducting risk assessment under article 35 of the GDPR' Phd thesis, Gottfried Wilhelm Leibniz Universität, 2021, ii, xxiii, 275 S. DOI: https://doi.org/10.15488/11364 (accessed 12 September 2023).

132 L Bygrave 'Hardwiring privacy' University of Oslo Faculty of Law Research Paper 2017-02. See also A Cavoukian 'Privacy by design: The 7 foundational principles' (2009, revised 2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (accessed 31 July 2019).

133 FRA *Handbook on European data protection law* (2018) 183-184. See also L Bygrave 'Data protection by design and by default: Deciphering the EU's legislative requirements' (2017) 4 *Oslo Law Review* 2; A Cavoukian 'Privacy by design: The 7 foundational principles', https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (accessed 30 March 2023).

134 B van Alsenoy 'Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 JIPITEC 271 para 1.

135 Alsenoy (n 134).

136 (1932) AC 562.

are entrenched throughout the AI system's life cycle. This, in turn, will ensure compliance with the duty of care and accountability principles.

Notably, irrespective of the discussion above, much responsibility still lies in the data protection supervisory authority, AI developers, controllers, processors, and other stakeholders to pursue privacy compliance on a large scale and to imbed such culture in the AI life cycle. For instance, even though there is a provision requiring a justifiable legal basis for personal data processing in the regulatory instruments considered in this article, the evidence suggests that AI developers do not comply with them. Therefore, regulatory intervention through guidelines, audits, robust whistle-blowing, and enforcement actions will be necessary to secure compliance.[137] In other words, mere reliance on the letters of the law would not yield any benefits without regulatory enforcement actions.

The findings of this article reveal that the NDPC is better suited to enforcing the privacy aspects of AI regulation. Section 5 of NDPA has assigned several functions to the Commission, including the power to regulate the deployment of technological measures to enhance personal data protection, investigate violations of data protection law, collaborate with other ministries and agencies, and carry out legal actions, among others. The NDPC can monitor and enforce data protection compliance within the AI sector if effectively utilised. Any aspect not adequately covered by data protection law, such as using biased data in AI, especially in the machine-learning phase, could be tackled in collaboration with other agencies through further regulatory guidance or legal reform. Although the data quality principle might curb the effects of data bias, additional regulatory guidance remains necessary.[138] It is suggested that law makers and ministers should be proactive and critically analyse all aspects of emerging technologies, including AI, in their functions. Although adopting a technology-neutral approach ensures the applicability of laws irrespective of the technology or activity being assessed, sometimes specific legislation is an excellent tool to address pressing needs.

7 Recommendations and conclusion

This article has examined key data protection issues around developing and deploying AI systems in Nigeria. It has highlighted the tensions between AI techniques and data protection principles. For example, AI systems rely heavily on large amounts of data for model training, and data repurposing is common. These features appear antithetical to data protection principles of data minimisation and purpose limitation. Issues around the legal basis for collecting data, data quality, transparency, data security, and automated decision making

137 Web scaping has been found to be a way through which AI developers collect large volumes of (personal) data (n 79).

138 Eg, AI could have an impact on labour rights where it is used as part of the recruitment process, or for measuring employee performance, etc. In such case, the Federal Ministry of Labour and Employment could team up with the NDPA to tackle the issue of AI in this respect.

have also been explored to demonstrate these challenges. Moreover, AI systems can perpetuate and even exacerbate existing biases in the data used to train the models, leading to discriminatory outcomes.

To address these concerns, some actions are needed in several areas, and the following recommendations are suggested towards addressing them:

(1) AI will have vast implications for Nigerian society, requiring a careful understanding of these impacts to integrate this technology safely and effectively. Therefore, the authorities should invest in AI governance research and ensure it has AI experts throughout this process of adopting a national AI policy. It is welcomed that the Federal Ministry of Communications, Innovations and Digital Economy is already thinking in this direction; it further recommended that this approach be augmented with an expert study on the impact of AI on human rights, particularly on privacy, in Nigeria. This will assist regulatory stakeholders in developing a comprehensive AI human rights framework grounded in global best practices. Given that the challenges posed by AI are global, such a framework should consider international standards, including a proactive, principled, and risk-based approach to AI regulation. This will offer a comparative advantage and position Nigeria at a vantage point to export its AI technology and take pride in developing responsible and ethical AI. Ultimately, the success of AI systems in Nigeria will depend on the regulatory ability to address the complex ethical, legal, and social issues that arise in their development and deployment.

(2) Besides developing a framework, enforcing data protection requirements should be at the forefront of Nigeria's data protection regime, particularly regarding AI. This incidentally will impact how AI developers and deployers consider data protection principles and obligations in their business. Enforcement should emphasise data collection processes, particularly in the machine learning phase, to ensure compliance with the legal basis for data processing requirements. The duty of care and accountability principles should also be effectively used during enforcement to interrogate whether the affected actors have taken reasonable standards of care regarding no harm to data subjects.

(3) Nigeria's AI policy should emphasise the use of privacy-enhancing mechanisms such as PIA and PbD as an integral part of the AI life cycle where such system is to be used to process personal data to ensure that data protection principles are enshrined and implemented throughout all AI-related data-processing activities. This will ensure that AI systems are designed to collect only the minimum amount of (personal) data needed for specific purposes and adhere to stated purposes. Furthermore, using industry standards should be strongly encouraged and recommended to AI system developers. These industry standards are essential because AI technical requirements may vary from industry to industry.

(4) Finally, until NDPR and NDPA are harmonised into a single framework, it is recommended that the regulatory stakeholders interpret and read them in a complementary fashion to address the gaps in each of them as they relate

to AI. In this respect, it is recommended that the NDPC critically review NDPR to address any gaps or conflicts with NDPA to avoid uncertainty.[139]

In conclusion, the proliferation of AI and its emergence as a reliable technology cannot be denied. However, it has also been shown that AI systems are fraught with potential privacy and data protection concerns that require all stakeholders' attention at the various stages of the AI life cycle. This article argues that effective privacy regulation of AI systems is crucial for safeguarding human rights, including the right to privacy and data protection. It also acknowledges the complexities and difficulties of regulating AI systems, particularly given the rapid pace of technological change and the potential for unintended consequences. These recommendations will go a long way in addressing these challenges.

139 Such a review may eventually lead to its repeal or update.