ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE, PRIVACY, AND DATA PROTECTION IN NIGERIA

BY

1. Oriko Blessing Chimaobi
Department Computer Science
Ebonyi State University

2. Dr. Nwoba Charles Chukwuma
Department of Political Science
Ebonyi State University

3. Onwa Doris Ogechi,
Department of Political Science
Ebonyi State University

4. Dr. Nwankwo Uchenna Oliver
Department of Political Science
Ebonyi State University

Abstract

Artificial intelligence (AI) governance, privacy, and data protection in Nigeria is increasingly becoming a critical area of focus for policymakers, businesses, and citizens alike. As AI technologies advance and become more integrated into various sectors, from healthcare to finance, the need for effective governance frameworks to manage these innovations has never been more pressing.This paper is on Artificial Intelligence (AI) Governance, privacy and data protection in Nigeria. An explorative study was adopted using literature review as the basis for information gathering. The study revealed that a balanced approach to governance, privacy, and data protection in Nigeria will not only bolster technological development but also safeguard the rights and freedom of its citizens. One important aspect of this governance involves the enforcement of data protection regulations that comply with global standards, such as the General Data Protection Regulation (GDPR). There is a concerted effort to establish local legislation that not only protects citizens' personal information but also fosters a conducive environment for technological advancement. This includes the need for strict guidelines on how data can be collected, stored, and utilized, ensuring informed consent is a priority in data transactions. Moreover, the ethical implications of AI systems must be at the forefront of governance discussions. Collaborative initiatives between government, academia, and industry leaders are crucial in addressing these challenges. Establishing multi-stakeholder forums can facilitate dialogue around best practices in AI governance, enabling a holistic approach to privacy and ethical considerations. Public engagement initiatives also play a critical role in raising awareness about data rights and empowering citizens to take an active stance in their digital privacy. In navigating these complexities, it is essential for the Nigerian government to adopt a proactive stance, ensuring that the legislative landscape evolves in tandem with the rapid advancements in AI technology. Ongoing assessments of AI systems through regular audits can enhance compliance with established norms, fostering public trust and promoting a more responsible approach to AI integration across the nation.

Keywords: Artificial Intelligence, governance, ethics, privacy, data protection

Introduction

As Nigeria strides towards becoming a leading player in the AI landscape, a judicious approach to governance, privacy, and data protection will not only enhance technological progress but also safeguard the rights and freedom of its citizens. The Global Privacy Assembly (GPA 2025) emphasized human oversight in AI decision-

making, highlighting risks of algorithmic bias and opaque systems. Countries like India and Nigeria are exploring governance models that integrate digital literacy, sustainability, and inclusivity. The governance of artificial intelligence, alongside privacy and data protection in Nigeria, necessitates a comprehensive and nuanced approach, particularly in light of the rapid advancements in technology and the concomitant challenges they present. The intricate interplay between legislative frameworks, ethical considerations, and technological innovation underscores the urgency of establishing robust governance mechanisms. The Joint Statement by 20 Data Protection Authorities (2025) stressed trustworthy data governance frameworks to protect privacy while enabling innovation. Africa's rapid digital transformation has heightened privacy concerns, leading to summits like the Data Protection Africa Summit 2025 in Ghana. Privacy-by-design principles are being embedded into AI systems to ensure compliance with GDPR and similar laws.

As Nigeria endeavors to harness the transformative potential of artificial intelligence, it must simultaneously address the paramount concerns surrounding individual privacy and the safeguarding of personal data. The proliferation of AI technologies has engendered a paradigm shift, necessitating a reevaluation of existing legal and regulatory structures to ensure they are adept at managing the complexities inherent in the digital landscape.

In recent years, there has been a burgeoning discourse on the ethical implications of AI deployment. Stakeholders, including policymakers, technologists, and civil society organizations, are increasingly advocating for a collaborative approach to governance that emphasizes transparency, accountability, and inclusivity (IBM AI Ethics Board Report 2025). This multifaceted dialogue is essential for cultivating a legal framework that not only protects citizens' rights but also promotes innovation and economic growth.

Moreover, the implementation of comprehensive data protection laws is imperative to fortify public trust in AI systems (Nigeria Data Protection Act (2025 amendments). The adoption of stringent measures to safeguard personal information will serve as a bulwark against potential abuses and will enhance the legitimacy of AI applications across various sectors. In this context, the establishment of independent oversight bodies is crucial to monitor compliance and address grievances arising from the misuse of data.

2. Literature Review

Conceptual Analysis

Artificial Intelligence Artificial intelligence (AI) is, simply put, a technology that allows machines and computer applications to mimic human intelligence, learning from experience via iterative processing and algorithmic training, it is a form of intelligence that is used to solve problems, come up with solutions, answer questions, make predictions, or offer strategic suggestions.(CSU Global, 2021). AI encompasses a wide range of technologies and applications, all aimed at enabling machines to perform tasks that typically require human intelligence. Systems with artificial intelligence use data and algorithms to function. First, in a procedure called training, vast amounts of data are gathered and fed into mathematical models, or algorithms, which utilise the data to identify patterns and provide predictions (Russell, S. J., and Norvig P.2020).

Data Protection

Data protection encompasses measures to safeguard data integrity, confidentiality, and availability against various threats such as cyberattacks, data breaches, and malicious activities (ISO/IEC 2022). Where vast amounts of data are generated, stored, and transmitted, ensuring robust data privacy and security measures is of utmost importance (Rao, et al 2023). These measures not only protect sensitive information but also uphold trust between organizations and their customers, comply with regulatory requirements, and mitigate financial and reputational risks associated with data breaches (Oluwatoyin et al 2024). Data protection is the duty of the organization, body or persons who collect data from another party, they are vested with the duty to protect the data being supplied by such other party from any use to which consent have not been given by the owner (NDPR 2019). Thus, where through the negligence or otherwise of the organization, data supplied by another party got used for a purpose for which it has not been approved, such organization may be liable to the extent of the use.

Data Privacy

To understand data privacy or data protection, it is imperative to have an understanding of what data is in this context. Data in this sense refers to a set of information about a person either expressly given or learnt through the activities engaged in by such person (GDPR, Article 4(1)). Data is given, for instance, when a person voluntarily supplies their information by filling out a form, through an interview or by publishing such information, it is learnt where a person's pattern of activities is used to determine some aspect of his life. Data privacy refers to the right of an individual to protect sensitive information about him or information which such individual wishes to protect from the public from unauthorised access, use, or disclosure, ensuring that individuals have control over their personal data (Chua et al., 2021).

The performance of the AI and the veracity of its outputs are directly influenced by the amount and quality of training data imputed (Russell & Norvig (2020). For AI to effectively learn and imitate patterns, they need large, diverse datasets. Depending on the application, the data might be anything from text and pictures to more intricate data types like biometric data. Although useful, there is an inherent risk to privacy when this data incorporates personal information and maintaining the delicate balance between innovation and security requires an understanding of the relationship between Artificial Intelligence (AI) and data privacy. (Academy of Management Review 2020). According to Nguyen (2024) explored the current context surrounding AI and privacy, and the importance of maintaining control over data, highlighting the importance of protecting individuals' sensitive information such as respecting individual rights, building trust and social acceptance, and in order to be in compliance with regulations. The author recommends potential solutions such as assessing the system's decision-making processes to identify any potential biases or errors, monitoring the AI system's accuracy and other attributes over time to help identify potential issues or deviations, and ensuring that the AI system is fair, unbiased, and effective in solving real problems. According to Cate and Dockery (2024) while compliance with existing data protection laws is important, it is imperative to confront the issue of privacy in the use of AI with a better long term approach which will be to see the challenges presented by AI as another wake-up call that our current approach to data protection is growingly outdated, archaic and

progressively ineffective. With this understanding, the author asserts that it is data protection law that must be improved if it is to protect privacy, effectively address the challenges presented by AI, and avoid creating unnecessary, bureaucratic barriers to AI's benefits. Rayhan and Rayhan (2023) conducted an in-depth study into the concept of AI and data privacy to understand the historical development of AI, its ethical implications, and the legal frameworks guiding its deployment. Using real-world case studies, their study analyzed instances where AI had both advanced and threatened human rights, one of such threats discussed is biases embedded in AI algorithms and that the reliance on biased historical data can perpetuate discrimination, leading to unfair treatment and decisions in various domains. The authors recommend the need for explainable and transparent AI, stressing the importance of ethically driven development and responsible deployment through a comprehensive re-examination of international and national regulatory efforts. Devineni (2024) explores the transformative impact of Artificial intelligence on data privacy and security by discussing traditional AI methodologies and their associated shortcomings. The discourse revolves around how AI with its 'automation and anomaly identification capabilities is transforming this field' and practical examples of real-world applications of AI in banking and health care to give an insight into how AI can be integrated into the security system, there are further discussions on ethical concerns that despite the immense benefits that may be derived from AI there is a significant concern on potential biases, surveillance energy as an issue and data handling issues is performed to have a comprehensive understanding of AI.

3. AI Ethics Principles and Controls that will ensure AI Governance, Privacy and Data Protection

Artificial Intelligence (AI) Ethics Principles and Controls are frameworks designed to ensure AI systems are developed and used responsibly, protecting human rights, privacy, and societal values. They combine high-level ethical principles with practical governance controls that organizations can apply across the AI lifecycle (UNESCO Recommendation on AI Ethics 2021).

1. **Fairness**: Fairness is a key principles ensuring that AI technologies treat all users equally and without bias. AI misleads all individually equitably without bias or discrimination. This ensures inclusive and outcomes across the society (UNESCO Recommendation on AI Ethics 2021).
2. **Privacy and Security:** Ensuring data protection is essential for maintaining user privacy and safeguarding sensitive information in AI applications. The framework emphasizes strong safeguards (OECD 2019).
3. **Humanity:** Respect human dignity, rights and cultural values in the design and use of AI. It is about designing systems that serve people not to replace or devalue them. AI should contribute to a greater goal enhancing society well being and to support a sustainable developments.
4. **Social and environmental benefits**: Promoting AI applications tat contribute positively to society and the environment. AI must be technically sound and dependable as well whether it's a healthcare algorithm or a smart intensity system. (UNESCO 2021)
5. **Reliability and safety:** Developing AI systems that are technically sound, dependable and safe to use. People should understand how AI systems work.(UNESCO 2021)

6. **Transparency:** it builds trust and helps users make informed decisions when in tract with the AI and it is not enough for AI to make decisions only when we need to know why. Transparency is a core principles ensuring that AI systems operate in an understandable manner.
7. **Explainability:** Make AI decisions and processes understandable and accessible to stakeholders. Explainability ensures that stakeholders can inteprete and challenge AI outcomes when necessary and behind every AI system are human choices, accountability ensures that individuals and organizations remain responsible for the ethical embark of the AI solution.(UNESCO 2021)

Privacy and Data Protection

In the age of AI data is power but with power comes with responsibility and one of the most pressed ethical concern we face today is privacy.

Data Privacy Challenges in AI

Some of the data privacy challenges in AI include the following

1. **Data Breaches:** Data breaches pose a significant risk to data privacy in AI applications, exposing sensitive information to unauthorized access. AI system often relies on massive dataset , many of which contain sensitive positive information of people or organizations that need to be kept private, but the more data we collect the greatest risk of exposure. Single breach can compromise not just privacy but trust as sell. And once the trust is broken it has to be rebuilt (NIST Cybersecurity Framework 2020)
2. **Unauthorized data usage:** It undermines trust in AI systems as personal data may be exploited without user's consent. Sometimes, data us repurposed but without the user knowledge or content may be it was collected for one initially purpose but it ends up being used for something entirely different as well like targeted advertising/surveillance. That kind of missue doesn't just affect privacy.it can elude confidence in AI itself (UNESCO 2021)
3. **Consent and Sensitive Information:** Collecting sensitive information without users' consent raises ethical concerns and challenges the integrity of AI practices. A lot of times users aren't fully informed about what data has been collected how it is being used and who has access to it. When AI systems handle deep personal data like health records biometric details transparency and concerns shouldn't be optional. Protecting prviacy in AI isn;'t just about compliance, its about respect for the individuals for their autonomy and for the trust they placed on the system we built. So how do we protect this information and still enabling innovation.

Strategies for Data Protection

1. **Data Anonymization**

Data anonymization removes personally identifiable information from data sets, helping to protect user privacy while enabling data analysis. This means striping a way boisterly identifiably information from dataset. Think of it like blurring of faces in a crowd photo, you will still get the big picture but no individual can be identified. It is a powerful way to preserver privacy while still keeping the data used for analysis (NIST Special Publication 800-53 2020)

2. Encryption Techniques

Implementing encryption techniques secures data by making it unreadable to unauthorized users, ensuring confidentiality and integrity. This is like locking your data in a digital way, think of it as turning your data into a secrete code only those

with authorization key can read it, it ensures that data even if it is intercepted it remains secured and confidential (NIST Special Publication 800-111 2007)

3. Access control:

we control access not everyone should see everything limiting access to who can have access to what data helps prevent misuse and breeds trust. Together these strategies form the ethical backbone of a responsible AI ensuring that innovation never comes at the cost of privacy. Strict access controls ensure that only authorized personnel can access sensitive data, minimizing risks of data breaches (NIST Special Publication 800-53 2020)

The Nigerian Data Protection Act (NDPA)

The NDPA was enacted to safeguard the fundamental rights and freedoms,and the interests of data subjects, to provide for the regulation of the processing of personal data; the promotion of data processing practices that safeguard the security of personal data and privacy of data subjects; to ensure that personal data is processed in a fair, lawful and accountable manner; to protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights; to ensure that data controllers and data processors fulfil their obligations to data subjects; to establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors; and to strengthen the legal foundations of the national digital economy (Nigeria Data Protection Act 2023). The Act is applicable to a controller who is resident in Nigeria and processes data in Nigeria or who neither resides in Nigeria nor processes data in Nigeria but processes data of Nigerians(Nigeria Data Protection Act 2023) The NDPA draws heavily from the European Union GDPR in terms of the rights of data subject and obligations of controller and processor. The Act provided for the rights of data to have their data protected and secured and the duties of controllers that collect and use data to protect such data. A controller of data is only allowed to process data lawfully, this means compliance with the provision of the regulation by being transparent, use for legitimate purposes only and collection of data that are only necessary and adequate. Processing is deemed to be lawful where such processing is done with the consent of the data subject, where it is necessary for compliance with legal obligation, to protect the interest of the data subject or a third party, or where it is necessary to process such data in the interest of the public.(Nigeria Data Protection Act 2023). Consent by the data subject is however not an absolute or total surrender of their interest in their personal data, the data subject retains the right to withdraw consent at any time, and the withdrawal shall not nullify any process that has been done by the controller or processor.(Nigeria Data Protection Act 2023) The controller on the other hand is obligated to ensure that the data subject is notified of the use to which the data will be put as the burden of proof rests on the data controller to establish that the data subject was notified.(Nigeria Data Protection Act 2023)

Conclusion

In conclusion, the governance of artificial intelligence in Nigeria, intertwined with the principles of privacy and data protection, is a pressing concern that requires immediate attention. By fostering a synergistic relationship between technological advancement and regulatory oversight, Nigeria can pave the way for a future where AI serves as a catalyst for positive societal transformation while upholding the fundamental rights of its citizens.

References

Academy of Management Review (2020): "The Dark Side of AI: Ethics, Privacy, and Security Risks"

Bloomberg Law, 'Is Biometric Information Protected by Privacy Law' (Bloomberg Law, 20 June 2024) https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/ accessed 24 June 2024.

Chi Nguyen, 'AI and Data Privacy: Balancing Innovation with Security' (2024) accessed 20 June 2024

Chua, H. N., Ooi, J. S., & Herbland, A. 'The effects of different personal data categories on information privacy concern and disclosure' (2021) Computers & Security, 110.

Cloudfare, 'What is NLP (Natural Language Processing?' https://www.cloudflare.com/learning/ai/natural language-processing-nlp/ accessed 25 August, 2024.

CSU Global, 'How Does AI Actually Work?' (CSU Global, 9 August 2021) accessed 18 June 2024.

Ellen Glover, 'Artificial Intelligence' (BuiltIn, 2 April 2024) < https://builtin.com/artificial-intelligence> accessed 18 June 2024

Fred H. Cate & Rachel Dockery, 'Artificial Intelligence and Data Protection: Observations on a Growing Conflict' accessed 20 June 2024.

GDPR (General Data Protection Regulation): EU regulation on personal data protection (Article 4(1))

ISO/IEC 27001:2022: Information security management systems

NDPR (Nigerian Data Protection Regulation) 2019: Nigerian regulation on data protection (Section 2, Section 3)

NIST Cybersecurity Framework (2020): Guidelines for managing cybersecurity risks, including data breaches

NIST Special Publication 800-111 (2007): Guide to Storage Encryption Technologies for End User Devices

NIST Special Publication 800-53 (2020): Security and Privacy Controls for Information Systems and Organizations.

OECD Principles on Artifical Intellgigence (2019): Principles 1.4 Data Protection and Privacy

Oluwatoyin Ajoke Farayola & Oluwabukunmi Latifat Olorunfemi & Philip Olaseni Shoetan, 'Data Privacy and Security in it: A Review of Techniques and Challenges' (2024) 5 (3) Computer Science & IT Research Journal

Rajan Rahan and Shahana Rahan, 'AI and Human Rights: Balancing Innovation and Privacy in the Digital Age' (2023) accessed 20 June 2024. 1-13

Rajan Rahan and Shahana Rahan, 'AI and Human Rights: Balancing Innovation and Privacy in the Digital Age' Op. cit

Rao, P. S., Krishna, T. G., & Muramalla, V. S. S. R., 'Next-Gen Cybersecurity for Securing Towards Navigating the Future Guardians of The Digital Realm (2023) 3 International Journal of Progressive Research in Engineering Management and Science, 178, 190.

Russell & Norvig (2020): "Artificial Intelligence: A Modern Approach" (Chapter 21, p. 733)

Russell, S. J., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

Shuroug, A. Alowais, 'Revolutionizing Healthcare: The Role of Artificial Intelligence in Clinical Practice' (2023) BMC Medical Education.

Siva Karthik Devineni, 'AI in Data Privacy and Security'(2024) 3 (1) International Journal of Artificial Intelligence & Machine Learning, pp. 35-49.

The UNESCO Recommendation on the Ethics of Artificial Intelligence was adopted in 2021,

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021): Principle 4 - Fairness and Non-Discrimination

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021): Principle 1 - Benefiting Humanity and the Environment

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021): Principle 7 - Transparency and Explainability, Principle 8 - Accountability

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021): Principle 7 - Transparency and Explainability.