IJAAR PUBLISHING®

Scholarly Journal of Advanced Legal Research | ISSN: 2782-8220
Vol. 6, Issue 1 (2026) | www.ijaar.org

Human Rights and Algorithmic Accountability under the Nigeria Data Protection Act 2023

By

Dr. Safiyyah Ummu Mohammed

Ag. HOD, Department of Public Law and Jurisprudence, Faculty of Law, Usmanu Danfodiyo University, Sokoto, Nigeria.

Abstract:

The Nigeria Data Protection Act 2023 (NDPA) establishes a foundation for data governance, but its capacity to ensure accountability for algorithmic decision-making is somewhat limited. Using a doctrinal research methodology, this article examines whether the NDPA adequately protects human rights against the distinctive harms of algorithmic systems such as opacity, bias, and diffusion of responsibility. It argues that while the NDPA provides essential data protection principles, it falls short in addressing certain human rights implications. Section 30 of the Act does not adequately deal with automated decision making, and there is also an absence of essential contestability mechanisms. The article recommends strengthening the right to human intervention, mandating fundamental human rights impact assessments and establishing independent oversight. Without these reforms, algorithmic systems may undermine the very rights the NDPA purports to protect.

Keywords: Algorithmic accountability, Nigeria Data Protection Act 2023, human rights, automated decision-making

https://doi.org/10.46654/6102-1848

1. Introduction

Algorithmic systems improve efficiency and decision making but also introduce risks to fundamental human rights. Concerns arise about the lack of transparency surrounding algorithmic processes and the difficulty of assigning responsibility when automated systems produce harmful outcomes. As algorithmic technologies become integrated into governance and commercial practices, questions of accountability and human rights protection have therefore become central to regulatory debates.

In Nigeria, algorithmic systems are deployed in sectors such as financial technology (fintech), telecommunications, digital platforms, and emerging forms of digital governance. Financial institutions rely on automated credit scoring tools, employers use digital platforms to filter job applicants, and online services deploy recommendation algorithms that shape access to information. These systems process large volumes of personal data and may significantly affect individuals' rights and interests. Yet the legal and institutional frameworks required to ensure accountability for algorithmic decision-making are still evolving.

The enactment of the Nigeria Data Protection Act 2023 (NDPA) marked a significant step in the country's data governance landscape. The Act establishes a statutory framework for the protection of personal data and creates the Nigeria Data Protection Commission (NDPC) as the primary regulatory authority. By codifying principles such as lawfulness, transparency, accountability, and data minimisation, the NDPA provides an important foundation for safeguarding informational privacy and regulating the activities of data controllers and processors. However, the ability of the NDPA to guarantee accountability for algorithmic decision-making remains uncertain. Algorithmic systems raise governance challenges that extend beyond traditional data protection concerns and individuals affected by algorithmic decisions may struggle to obtain explanations, challenge adverse outcomes, or secure effective remedies.

When viewed through the lens of human rights law, certain rights may be directly affected by algorithmic systems that process personal data and generate decisions. International human rights norms impose obligations on states to protect individuals from direct state interference harms caused by private actors operating within their jurisdiction. Consequently, regulatory frameworks governing data and digital technologies must be capable of addressing the risks posed by algorithmic systems.

This article therefore examines whether the NDPA provides an adequate framework for ensuring algorithmic accountability consistent with human rights standards. It focuses particularly on the Act's provisions relating to automated decision-making, transparency, and regulatory enforcement. The analysis identifies key limitations within the NDPA framework, including the ambiguity surrounding the right to human intervention, the absence of clear mechanisms for contesting algorithmic logic, and the institutional challenges associated with auditing complex automated systems.

The article begins with a conceptual and theoretical framework, examining the nature of algorithmic harm, the distinction between responsibility and accountability, and the relevance of international human rights law. The subsequent section analyses the relationship between algorithmic systems and fundamental rights within the Nigerian constitutional context, with particular emphasis on the rights to privacy and fair hearing. The article then evaluates the NDPA 2023 as Nigeria's primary legislative response to the governance challenges posed by algorithmic decision-making. Finally, it proposes recommendations aimed at strengthening algorithmic accountability within Nigeria's data protection regime.

2. Conceptual Framework and Literature Review

2.1 The Nature of Algorithmic Harm

Algorithmic systems possess unique characteristics that create challenges for human rights protection. Several features of these systems make them qualitatively different from traditional forms of decision-making.[1] First, many algorithms operate with a significant degree of opacity due to the complexity of machine learning models, the proprietary interests of companies that develop them, and the nature of algorithms that learn and change over time.[2] Even when developers intend to create transparent systems, the internal logic of advanced algorithms may exceed human comprehension.[3] Opacity is important because it becomes impossible to challenge a decision when the process of reaching that decision cannot be examined.

Algorithms are also dependent on data. They learn from historical data, which can contain biases reflecting existing social inequalities.[4] An algorithm trained on data from a society with a history of discrimination will likely reproduce, and may even amplify, those patterns. This is a structural feature of systems that learn from the past to make predictions about the future.

Furthermore, algorithms operate at scale. This means that any harm from a biased algorithm goes beyond a limited number of people and can affect millions of people. This can result in widespread discrimination. Algorithmic systems also involve distributed agency. Responsibility for an algorithmic decision is spread across many actors: those who conceive the system, those who write the code, those who supply the training data, those who deploy it, and those who use its outputs.[5]When something goes wrong, no single actor may feel responsible, and traditional legal doctrines built around individual fault may struggle to assign accountability.

2.2 Responsibility and Accountability

Responsibility refers to the function of absorbing uncertainty in decision-making. When a person or system processes information and produces an output that guides action, they assume responsibility.[6] Similarly, algorithms take on responsibility by taking data, applying rules and generating decisions. Accountability on the other hand refers to the obligation to explain and justify decisions, and to bear the consequences when things go wrong.[7] When algorithms replace humans, accountability becomes difficult to assign. This leads to an accountability gap that must be addressed through regulatory frameworks.

2.3 International Human Rights Law as a Framework

If algorithms cannot be held accountable, and responsibility is fragmented, individuals harmed by algorithmic decisions can seek redress through the framework of international

[1]Besio, C, Fedtke, C, Grothe-Hammer, M, Karafillidis, A &Pronzini, A 2025, 'Algorithmic responsibility without accountability: Understanding data-intensive algorithms and decisions in organisations', Systems Research and Behavioral Science, vol. 42, no. 3. 741.
[2] Pasquale, F 2015, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge, MA. 3.
[3] Burrell, J 2016, 'How the machine "thinks": Understanding opacity in machine learning algorithms', Big Data & Society, vol. 3, no. 1. 5.
[4] Noble, SU 2018, Algorithms of Oppression: How Search Engines Reinforce Racism, NYU Press, New York.
[5]Besio et al. n 1, 742.
[6]Ibid,743.
[7]Ibid,744.

human rights law, a product of decades of global consensus.[8] This provides a set of standards that can guide action across jurisdictions and sectors. The Universal Declaration of Human Rights and other treaties articulate rights that can be applied to algorithmic systems. For instance, Article 12 guarantees the right to privacy, threatened by mass data collection and algorithmic surveillance.[9] Article 2 guarantees non-discrimination, threatened by biased algorithms that perpetuate inequality.[10] Articles 8, 9, and 10 guarantee fair trial and effective remedy, threatened by unclear decisions that cannot be challenged.[11] These rights and others impose binding obligations. States must therefore refrain from violating rights and also protect individuals from rights violations by third parties, including businesses.[12] This requires the establishment of effective regulatory frameworks.

The UN Guiding Principles on Business and Human Rights further elaborate the responsibilities of private actors.[13] Businesses have an independent responsibility to respect human rights, which requires them to identify and mitigate potential harms before they occur, and providing remedies when harms occur despite their efforts.[14]

2.4 The Concept of Vulnerability

Algorithmic harms are not evenly distributed, resulting in some groups facing greater risks. The idea of vulnerability serves as a tool for determining which groups are most exposed to risk and the underlying reasons for such exposure. With algorithmic systems, vulnerability may arise from many factors, including technologies that fail to reflect population diversity, limited understanding of how algorithms operate, insufficient participation in decisions regarding their deployment, weak enforcement frameworks and a lack of resources to obtain remedies. These conditions tend to impact ethnic minorities, women, persons with disabilities, individuals with low income and people residing in rural areas with inadequate digital infrastructure.

3. Algorithms and Fundamental Rights in Nigeria

Within the Nigerian context, two rights protected by the 1999 Constitution of the Federal Republic of Nigeria are most susceptible to algorithmic harm. These are the right to privacy and the right to fair hearing. For each right, the analysis considers how algorithmic systems threaten its enjoyment and why existing protections may be insufficient.

3.1 Right to Privacy

Section 37 of the 1999 Constitution guarantees the right to privacy of citizens, their homes, correspondence, and telephone conversations. This right, like the right to privacy under international human rights law, protects individuals from arbitrary interference with their personal information and private life.[15] This right is threatened by Algorithmic systems in different ways. Facial recognition technologies, predictive analytics, and profiling systems require vast amounts of personal data to function. When deployed in public spaces or through

[8]Donahoe, E & Metzger, MMD 2019, 'Artificial intelligence and human rights', Journal of Democracy, vol. 30, no. 2. 116. McGregor, L, Murray, D & Ng, V 2019, 'International human rights law as a framework for algorithmic accountability', International and Comparative Law Quarterly, vol. 68, no. 2. 311
[9]Ibid, 329.
[10]Ibid.
[11]Ibid.
[12] McGregor et al n 8, 327.
[13] UN Human Rights Council 2011, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc HR/PUB/11/04.
[14]McGregor et al. n 8.
[15]Donahoe, E & Metzger, n 8, 120.

digital platforms, these systems can track movement, behaviours, and associations without consent. Algorithms can also obtain sensitive information from innocent data. This means that even when individuals consent to the collection of certain information, algorithms may generate new inferences that reveal personal details. For instance, algorithms can deduce political opinions, health status, or other protected characteristics from shopping patterns or social media activity.[16] Algorithmic systems can also operate across borders, with data processed in multiple jurisdictions.

In Nigeria, Fintech applications collect extensive personal data to make automated credit decisions. Also social media platforms used by millions of Nigerians employ algorithms that profile users for advertising and content curation. Although the NDPA provides some important protections such as requirements for lawful processing and data security, the provisions may not fully address the unique privacy challenges posed by algorithmic systems.

3.2 Right to Fair Hearing

Section 36 of the 1999 Constitution guarantees the right to fair hearing, including the right to be heard and the right to a reasoned decision. This right is fundamental to the rule of law: when the state makes decisions affecting individuals, those individuals must be able to understand and challenge the basis for those decisions.[17] Algorithmic systems threaten this right through opacity. When decisions about benefits, employment, or even criminal justice are informed or determined by algorithms whose logic is inaccessible, individuals cannot meaningfully challenge those decisions.[18]

In Nigeria, algorithmic systems are increasingly used in contexts that affect individuals' rights and interests. Banks use algorithms to make credit decisions. Employers use automated tools to screen job applicants. Government agencies may use algorithms to determine eligibility for services or benefits.[19] In each case, the right to fair hearing requires that affected individuals understand the basis for decisions and have a meaningful opportunity to challenge them.

The NDPA's Section 30 provides a right not to be subject to solely automated decisions and a right to human intervention. But as Section 4 will argue, these provisions may not be sufficient to guarantee fair hearing if "human intervention" means merely rubber-stamping algorithmic outputs, and if individuals have no right to understand the logic behind the decision.

4. The Data Protection Act 2023

The NDPA represents a significant milestone in the country's data governance framework. The Act establishes a statutory basis for data protection and creates the NDPC.

4.1 Overview of the NDPA 2023

The NDPA 2023 establishes a comprehensive data protection framework modelled in part on the European Union's General Data Protection Regulation (GDPR). It sets out principles for lawful processing of personal data, creates rights for data subjects, and establishes the NDPC as an independent regulatory authority with powers of investigation and enforcement.

[16] McGregor et al, n8, 316.
[17] Donahoe& Metzger, n 8, 120.
[18] Besio, C et al, n 1. 747.
[19] Aloamaka, PC &Omozue, MO 2024, 'AI and human rights: Navigating ethical and legal challenges in developing nations', KhazanahHukum, vol. 6, no. 2. 193.

The Act applies to data controllers and processors operating in Nigeria or processing personal data of data subjects in Nigeria.[20] The NDPA's core principles include lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.[21] These principles, provide a foundation for protecting individuals' information but are insufficient to address the unique challenges of algorithmic decision making.

4.2 Automated Decision-Making

Section 30 of the NDPA is the provision most directly relevant to algorithmic accountability and provides that "A data subject shall not be subject to a decision based solely on automated processing of personal data which produces legal effects concerning the data subject or significantly affects the data subject."[22]

However, automated decisions are permitted where they are necessary for entering into or performing a contract, authorised by law or based on explicit consent.[23] In such cases, data controllers must implement measures to safeguard the rights, freedoms and legitimate interests of the data subject. Yet, there is no explicit requirement that data subjects receive an explanation of how an automated decision was reached. This contrasts with the obligations in Section 24, which require controllers to provide meaningful information about the logic involved in processing.[24]

This is significant because if an individual cannot understand why a particular decision was made they cannot meaningfully exercise their right to contest that decision.[25] Section 30 requires that data subjects have the right to obtain human intervention, but there are no clear guidelines for this. According to the European Data Protection Board, human intervention must be meaningful, involving someone with the authority and competence to actually change the decision.[26] The NDPA does not provide such guidance, leaving the meaning of this safeguard subject to interpretation. Furthermore, there is no mechanism for contesting the logic, only the outcome. Section 30 allows individuals to contest the decision, but it does not provide a mechanism for challenging the algorithm itself. If an individual believes that an algorithm is systematically biased or fundamentally flawed, they have no basis under Section 30 to challenge its design or deployment.[27]

4.3 Data Protection Impact Assessments

Section 37 of the NDPA requires data controllers to conduct a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of data subjects.[28] The assessment must include a systematic description of the processing and assessments of necessity and proportionality, risks to rights and freedom and measures to address those risks.[29] However, there is no explicit requirement to assess impacts human rights that algorithmic systems may affect.

[20]NDPA, s 2.
[21]Ibid, Second Schedule, Part 1
[22]Ibid, s 30(1).
[23]Ibid, s 30(2
[24]Ibid, s 24(1)(a).
[25]McGregor, L, Murray, D & Ng, V 2019, n8. 335.
[26] European Data Protection Board 2018, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01, para 21
[27]McGregor et al., 'International human rights law as a framework', p. 340.
[28]NDPA, s 37(1)
[29]Ibid, s 37(2

4.4 Enforcement and Remedies

The NDPA establishes the NDPC as an independent regulatory authority with powers to investigate complaints, conduct audits, and impose administrative fines. Sections 47 to 53 set out the Commission's enforcement powers and the remedies available to data subjects. Data subjects may lodge complaints with the NDPC, which must investigate and issue a determination. The Commission may order the controller to take steps to comply with the Act, including ceasing processing or taking other specified actions. Data subjects may also seek judicial remedies, including compensation for damages suffered.

However, auditing algorithmic systems requires specialised expertise and complaints about algorithmic decisions will depend on whether recruited staff possess skills or can access external expertise. Also, for complaint mechanisms to be effective, subjects must have certain level of awareness, literacy, and resources. Individuals who do not know that an algorithm affected them, who cannot afford legal representation, or who lack access to the internet may be effectively excluded.[30]

5. Recommendations

i. Section 30 of the NDPA is the cornerstone of algorithmic accountability, but its provisions require clarification and strengthening to include an explicit right to a meaningful explanation. Individuals subject to automated decisions should receive not merely information about how the system works in general, but an explanation of why a particular decision was reached in their case. This explanation must be accessible to people without technical expertise and also provide enough detail to enable challenges.

ii. The right to human intervention is meaningless if the human merely rubber-stamps algorithmic outputs. Intervention must involve a reviewer with authority to override the decision, and access to all information considered by the algorithm

iii. A mechanism to challenge algorithmic logic, not merely outcomes must be developed. Individuals should be able to raise complaints about both systemic issues and individual decisions. This could be achieved through a provision allowing representative actions by civil society organisations or through empowering the NDPC to investigate systemic concerns on its own initiative.

iv. The NDPA's requirement for Data Protection Impact Assessments is valuable but insufficient. Nigeria should mandate Fundamental Rights Impact Assessments (FRIAs) for high-risk algorithmic systems. Assessments should explicitly evaluate impacts on Privacy and data protection, fair hearing and due process as well any other relevant rights. FRIAs should be submitted to an independent oversight body for review before deployment.

v. Effective enforcement requires institutions with the technical expertise and legal authority to audit complex algorithmic systems. A dedicated algorithmic accountability unit within the NDPC should be established. This unit should be staffed with experts that can issue guidance on algorithmic accountability and investigating systemic concerns. It should also be empowered with legal authority to issue binding orders and impose sanctions for non-compliance.

[30] Aloamaka, PC & Omozue, MO n 19. 197.

6. Conclusion

The use of algorithmic systems has created challenges for the protection of fundamental rights. While these technologies promise efficiency and innovation, they also introduce risks that traditional legal frameworks were not designed to address. Lack of transparency, bias and the diffusion of responsibility across multiple actors make algorithmic decision-making particularly difficult to regulate through conventional mechanisms. In such circumstances, individuals affected by automated decisions may find it difficult to understand, challenge, or obtain remedies for decisions that significantly affect their rights and interests.

Nigeria's adoption of the Nigeria Data Protection Act 2023 represents an important milestone in the development of a modern data governance framework. By establishing statutory data protection principles and creating the Nigeria Data Protection Commission, the Act provides a legal foundation for regulating the processing of personal data and safeguarding informational privacy. Its recognition of automated decision-making and the right to human intervention demonstrates an emerging awareness of the risks associated with algorithmic systems.

However, the analysis in this article shows that the NDPA does not yet provide a comprehensive framework for algorithmic accountability. The provisions governing automated decision-making remain limited in scope and leave significant interpretive gaps. In particular, the absence of a clear right to a meaningful explanation of automated decisions, the lack of mechanisms to challenge the design or logic of algorithmic systems, and the uncertainty surrounding the nature of human intervention weaken the effectiveness of the safeguards provided. In addition, the capacity of regulatory institutions to audit complex algorithmic systems and investigate systemic harms remains an important concern.

Addressing these challenges requires a more explicit integration of human rights principles into Nigeria's data governance framework. Regulatory mechanisms must ensure that individuals subject to automated decisions can understand how those decisions were made, contest them effectively, and obtain remedies where harm occurs. Strengthening impact assessment requirements, clarifying the obligations of data controllers, and enhancing the technical capacity of the Nigeria Data Protection Commission are essential steps in this process.

Finally, algorithmic systems should not operate beyond the reach of legal accountability. As these technologies become increasingly embedded in economic and governmental decision-making, regulatory frameworks must evolve to ensure that technological innovation does not undermine fundamental rights. Strengthening the human rights safeguards within the NDPA will therefore be crucial to ensuring that algorithmic governance in Nigeria develops in a manner consistent with the principles of transparency, accountability, and the rule of law.

REFERENCES

[1] Aloamaka, PC & Omozue, MO 2024, 'AI and human rights: Navigating ethical and legal challenges in developing nations', Khazanah Hukum, vol. 6, no. 2. 189-201.

[2] Besio, C, Fedtke, C, Grothe-Hammer, M, Karafillidis, A & Pronzini, A 2025, 'Algorithmic responsibility without accountability: Understanding data-intensive algorithms and decisions in organisations', Systems Research and Behavioral Science, vol. 42, no. 3, pp. 739-755

[3] Burrell, J 2016, 'How the machine "thinks": Understanding opacity in machine learning algorithms', Big Data & Society, vol. 3, no. 1, pp. 1-12.

[4] Donahoe, E & Metzger, MMD 2019, 'Artificial intelligence and human rights', Journal of Democracy, vol. 30, no. 2, pp. 115-126; McGregor, L, Murray, D & Ng, V 2019, 'International human rights law as a framework for algorithmic accountability', International and Comparative Law Quarterly, vol. 68, no. 2, pp. 309-343.

[5] McGregor, L, Murray, D & Ng, V 2019, 'International human rights law as a framework for algorithmic accountability', International and Comparative Law Quarterly, vol. 68, no. 2, p. 316.

[6] Noble, SU 2018, Algorithms of Oppression: How Search Engines Reinforce Racism, NYU Press, New York.

[7] Pasquale, F 2015, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge, MA.

[8] UN Human Rights Council 2011, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc HR/PUB/11/04.