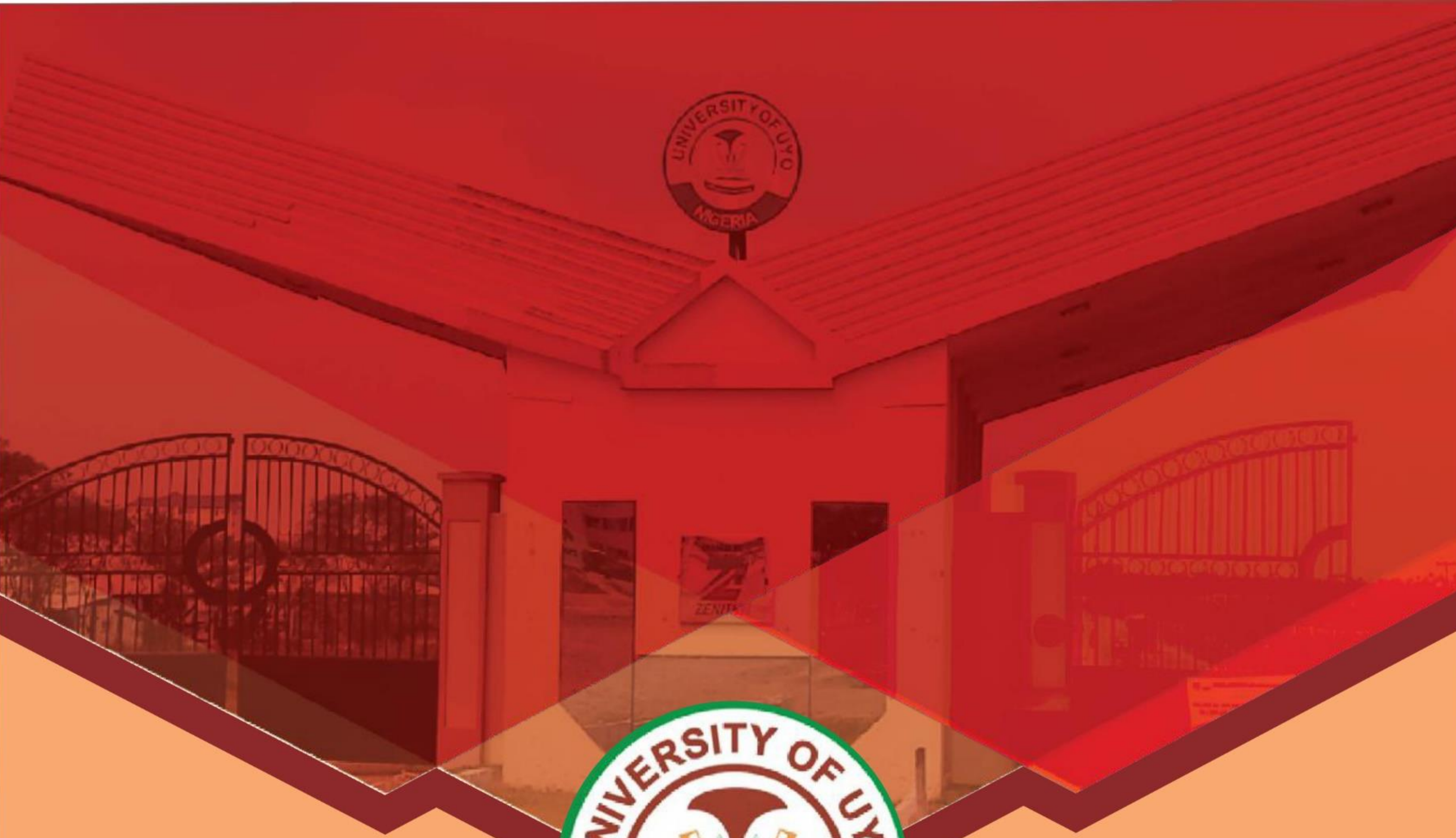

UNIVERSITY OF UYO LAW JOURNAL

VOLUME 13 (2025)

Published by the Faculty of Law
University of Uyo, Nigeria

Artificial Intelligence Surveillance in Nigeria: Finding the Sweet Spot between National Security, Data Protection and Digital Rights

E. A. Essang, Esq.[*]

Abstract

This paper examines the deployment of AI-powered surveillance in Nigeria, focusing on the need to balance national security with digital rights and data protection. It explores the existing legal and regulatory frameworks governing surveillance technologies, assesses their implications for individual rights, and identifies challenges and opportunities for achieving a balanced approach. Using a doctrinal method, the paper analyses Nigerian laws, policies, and regulations relating to surveillance, data protection, and digital rights, while drawing on international human rights instruments and best practices in AI-powered surveillance. The study reveals that Nigeria's regulatory framework is inadequate and fragmented, leaving significant gaps in the protection of citizens' digital rights and personal data. It further observes that the increasing use of AI-powered technologies enables extensive surveillance of citizens, posing serious risks to freedoms of expression, association, and assembly. The paper identifies challenges such as lack of transparency and accountability in surveillance operations, weak data protection mechanisms, and low public awareness of digital rights. It recommends the enactment of comprehensive legislation on AI-powered surveillance and data protection, the establishment of an independent oversight body to ensure accountability, and emphasises the need for enhanced citizen education and institutional capacity-building for effective rights protection.

[*] LLB [Uniuyo], BL [Abuja], LLM [RSU], Doctoral Researcher, Rivers State University, APLA Researcher, Oil, Investment, Gas, Mineral, and Environmental Law Researcher, National Secretary, Association of Environmental Lawyers of Nigeria, Chartered Green Advocate of Nigeria, email: edemumohessang@gmail.com; +2348128710639.

University of Uyo Law Journal Volume 13 (2025): 93-108

Keywords: AI-Powered, Surveillance, Data Protection, National Security and Digital Rights

1. Introduction

The rapid advancement of technology and the widespread use of the internet, social media, and mobile devices have raised significant concerns about the protection of the right to privacy in Nigeria. Despite the guarantees provided by Section 37 of the Constitution of the Federal Republic of Nigeria, 1999, which protects the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications, the right to privacy remains under threat in the digital age.[1] The problem is exacerbated by the lack of comprehensive legislation on data protection in Nigeria. While the Nigeria Data Protection Act, 2023, has been criticized for its limitations. For instance, it does not provide adequate safeguards against the collection and use of personal data by government agencies. Furthermore, the Act does not provide clear guidelines on the right to erasure, the right to data portability, and the right to object to processing. However, section of NDPA, 2023 provides that the Act shall safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, ensure that personal data is processed in a fair, lawful and accountable manner.[2]

Additionally, the NDPA, 2023, provides for data processing practices that safeguard the security of personal data and privacy of data subjects, protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights, ensure that data controllers and data processors fulfil their obligations to data subjects.[3] The use of surveillance technologies dates to the colonial era in Nigeria, where the British colonial authorities employed various forms of surveillance to maintain control and suppress dissent.[4] However, with the advent of artificial intelligence and other digital technologies, surveillance has become more sophisticated, and potentially invasive. Today, AI-

[1] Constitution of the Federal Republic of Nigeria, 1999 (as amended), s 37.

[2] Nigeria Data Protection Act, 2023, s 1 (a) (d).

[3] Ibid, s 1 (c-g).

[4] A Odusote, 'Data Misuse, Data Theft and Data Protection in Nigeria' [2021] (12) Beijing Law Review 1284-1298.

powered surveillance is increasingly being deployed in Nigeria, ostensibly to enhance national security and combat crime.[5]

The legal framework governing surveillance in Nigeria is fragmented and inadequate. The 1999 Constitution of the Federal Republic of Nigeria guarantees the right to privacy, but this right is not absolute and can be derogated from in certain circumstances. The National Security Agencies Act, 1987 (as amended) and the Terrorism (Prevention) Act, 2011 (as amended) provide some legal basis for surveillance, but these laws are often vague and overly broad, allowing for abuse and arbitrary application. In recent years, Nigeria has witnessed a significant increase in the deployment of AI-powered surveillance technologies, including facial recognition systems, biometric data collection, and social media monitoring. While these technologies have potential benefits for national security and crime prevention, they also pose significant risks to digital rights and data protection.[6] The lack of transparency and accountability in surveillance practices, combined with inadequate data protection laws and regulations, has created a perfect storm of risks for Nigerian citizens.[7] The Nigerian government has argued that AI-powered surveillance is necessary to combat terrorism, kidnapping, and other serious crimes. However, critics argue that these measures are often disproportionate and discriminatory, targeting specific communities and groups. Moreover, the use of AI-powered surveillance has been linked to various human rights abuses, including arbitrary detention, torture, and extrajudicial killings.[8]

The deployment of AI-powered surveillance in Nigeria poses significant risks to digital rights and data protection, while also raising concerns about national security and the rule of law. The lack of transparency and accountability in surveillance practices, combined with inadequate data protection laws and regulations, has created a situation

[5] Ibid.

[6] E Kolawole, 'Protecting Personal Data in Nigeria: An Examination of the Nigeria Data Protection Regulation 2019' [2020] (1) Journal of Intellectual Property and Digital Law 12-25.

[7] Ibid.

[8] E Kolawole, 'Protecting Personal Data in Nigeria: An Examination of the Nigeria Data Protection Regulation 2019' [2020] (1) Journal of Intellectual Property and Digital Law 12-25.

where Nigerian citizens are vulnerable to abuse and exploitation.[9] Therefore, there is a need to balance national security concerns with digital rights and data protection, and to develop a comprehensive legal and regulatory framework that governs AI-powered surveillance in Nigeria. Artificial Intelligence (AI)-powered surveillance has become increasingly prevalent in Nigeria, with the government and private sector deploying various technologies to monitor and track individuals. These technologies include facial recognition systems, biometric data collection, social media monitoring, and predictive policing. The use of AI-powered surveillance in Nigeria is often justified as a necessary measure to combat crime, terrorism, and other national security threats.

The Nigerian government has invested heavily in AI-powered surveillance technologies, with the National Intelligence Agency and the Department of State Services being major beneficiaries.[10] These agencies have deployed AI-powered surveillance systems to monitor public spaces, borders, and critical infrastructure. Additionally, the Nigerian Police Force has established a digital forensic laboratory to analyse digital evidence and track cybercrime. Private companies are also playing a significant role in the development and deployment of AI-powered surveillance technologies in Nigeria. Companies such as ZTE and Huawei have partnered with the Nigerian government to provide AI-powered surveillance solutions.[11] These solutions include smart city initiatives, which integrate AI-powered surveillance with other technologies such as Internet of Things sensors and data analytics.[12]

The rapid advancement of technology in the digital age has raised significant concerns about the protection of individuals' right to privacy. The widespread use of the internet, social media, and mobile devices has made it easier for governments, corporations, and individuals to collect, store, and share personal data, often without consent or transparency. This has led to surge in privacy violations, including data breaches, surveillance, and identity theft, which can have severe consequences for individuals, including reputational damage, financial loss, and emotional distress.

[9] A Makinwa, 'The Right to Privacy in Nigeria: A Critical Analysis of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015' [2022] (20) African Journal on Human Rights 301-321.

[10] Ibid.

[11] Ibid.

[12] Ibid.

The Nigerian Constitution, specifically, section 37 guarantees the right to privacy, stating that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected. However, the Constitution does not provide clear guidelines on how this right should be protected in the digital age. Furthermore, existing laws and regulations, such as the Cybercrime (Prohibition, Prevention, etc.) Act, 2015, have been criticized for being inadequate and inconsistent with international human rights standards. This has created a legal vacuum that allows for the exploitation of personal data and the erosion of individuals' right to privacy. Additionally, lack of effective protection for the right to privacy in the digital age has significant implications for Nigerian citizens, including the potential for abuse of power, suppression of free speech, and erosion of trust in institutions.

Despite the potential benefits of AI-powered surveillance, there are concerns about its impact on human rights and civil liberties in Nigeria. The use of AI-powered surveillance has been linked to arbitrary detention, torture, and extrajudicial killings. Additionally, there are concerns about the lack of transparency and accountability in the deployment of AI-powered surveillance technologies, as well as the potential for bias and discrimination. The deployment of AI-powered surveillance in Nigeria is governed by a patchwork of laws and regulations, including the National Security Agencies Act, 1986, the Terrorism (Prevention) Act, 2011 (as amended) and the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. However, these laws are often vague and overly broad, allowing for abuse and arbitrary application. As a result, there is a need for a more comprehensive and nuanced regulatory framework to govern the use of AI-powered surveillance in Nigeria.

2. Conceptual Clarification

i. Digital Age

The digital age refers to the current era of widespread use of digital technologies, including the internet, mobile devices, social media, and other digital platforms.[13] This era has been characterized by the rapid

[13] A A Oyediran, 'Data Privacy in Nigeria: Challenges and Prospects' [2020] (10) (2) Journal of Information Technology and Socio-Economic Technology 1-15.

advancement of technology, which has transformed the way people communicate, interact, and access information. In Nigeria, the digital age has led to an increase in the use of digital technologies, with over 100 million Nigerians having access to the internet and millions more using mobile devices and social media.[14] The digital age has also led to the emergence of new forms of data collection, storage, and dissemination. Personal data is now collected and processed on a massive scale, often without the knowledge or consent of the individuals concerned. This has raised significant concerns about the protection of the right to privacy, as individuals are increasingly vulnerable to data breaches, cybercrime, and online harassment.

ii. Privacy

Privacy refers to the state of being free from unauthorized intrusion, observation, or surveillance. It involves the right to control one's personal information, including sensitive data such as financial information, health records, and personal communications.[15] In the context of the digital age, privacy encompasses not only physical spaces, but also online activities, digital communications, and personal data stored on digital devices. In Nigeria, the concept of privacy is deeply rooted in the country's cultural and social norms. The idea of "private life" is highly valued, and individuals expect to have a reasonable level of control over their personal information and private spaces. However, the digital age has introduced new challenges to the concept of privacy, as personal data can be easily collected, stored, and disseminated online. This has raised concerns about the erosion of privacy and the potential for abuse of personal information.[16]The Nigerian Constitution recognizes the importance of privacy, guaranteeing the right to privacy in Section 37.[17] This provision protects the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. However, the interpretation and application of this

[14] Ibid.

[15] O A Dada, 'Data Protection and Privacy in Nigeria: An Examination of the Nigeria Data Protection Regulation 2019' [2020] (12) (1) African Journal of Information and Communication 1-18.

[16] O A Dada, 'Data Protection and Privacy in Nigeria: An Examination of the Nigeria Data Protection Regulation 2019' [2020] (12) (1) African Journal of Information and Communication 1-18.

[17] CFRN, 1999 (as amended).

provision in the digital age remain unclear, and the study aims to provide a constitutional analysis of the right to privacy in Nigeria's digital age.

3. National Security Concerns and Justification for AI-powered Surveillance in Nigeria

Nigeria faces numerous national security challenges, including terrorism, kidnapping, armed robbery, and cybercrime. The Boko Haram insurgency in the Northeast, for instance, has resulted in thousands of deaths and displacements, while kidnapping and armed robbery have become rampant in many parts of the country.[18] These security challenges have created a sense of urgency and necessitated the deployment of innovative technologies, including AI-powered surveillance, to enhance national security.[19] The Nigerian government has justified the deployment of AI-powered surveillance on the grounds that it is necessary to prevent and combat crime, as well as to protect national security.[20] The government has argued that AI-powered surveillance can help to identify and track criminals, anticipate and prevent crime, and improve the overall effectiveness of law enforcement agencies.[21] Additionally, the government has claimed that AI-powered surveillance can help to protect critical infrastructure, such as airports, seaports, and public buildings, from terrorist attacks and other security threats.[22]Therefore, one of the key national security concerns that AI-powered surveillance is intended to address is the threat of terrorism. Nigeria has been plagued by terrorist attacks in recent years, particularly in the Northeast, where Boko Haram has been active. AI-powered surveillance can help to identify and track terrorists, anticipate and prevent terrorist attacks, and improve the overall effectiveness of counter-terrorism operations.[23] Additionally, AI-powered

[18] A Adekunle, 'Data Protection and the Right to Privacy in Nigeria' [2019] (38) Nigerian Journal of Technology 123-135.

[19] O Olasoji, 'The Nigeria Data Protection Regulation 2019: A Critical Analysis' [2020] (1) Journal of Law and Technology 34-49.

[20] Ibid.

[21] O A Dada, 'Data Protection and Privacy in Nigeria: An Examination of the Nigeria Data Protection Regulation 2019' [2020] (12) (1) African Journal of Information and Communication 1-18.

[22] Ibid.

[23] Ibid.

surveillance can help to identify and disrupt terrorist financing networks, which are critical to the survival and operations of terrorist groups.[24]

Another national security concern that AI-powered surveillance is intended to address is the threat of cybercrime.[25] Nigeria has been identified as one of the countries most affected by cybercrime, with millions of Nigerians falling victim to cybercrime every year.[26] AI-powered surveillance can help to identify and track cybercriminals, anticipate and prevent cybercrime, and improve the overall effectiveness of cybersecurity operations.[27] Additionally, AI-powered surveillance can help to identify and disrupt cybercrime networks, which are critical to the survival and operations of cybercriminal groups.[28] The deployment of AI-powered surveillance in Nigeria is justified on the grounds of national security concerns, including the threat of terrorism, kidnapping, armed robbery, and cybercrime.[29] AI-powered surveillance can help to identify and track criminals, anticipate and prevent crime, and improve the overall effectiveness of law enforcement agencies.[30] However, it is also important to ensure that AI-powered surveillance is deployed in a manner that respects human rights and civil liberties, and that is transparent, accountable, and subject to oversight and regulation.[31]

4. Impact of AI Surveillance on Digital Rights and Data Protection in Nigeria

The deployment of AI-powered surveillance in Nigeria has significant implications for digital rights in the country. One of the major concerns is the potential for mass surveillance, where the government and other actors can monitor the online activities of citizens without their

[24] (n 13).

[25] I Ekoja, 'Digital Rights and Data Protection in Nigeria: Challenges and Prospects' [2020] (1) Journal of Digital Rights 12-28.

[26] E O Adebayo, 'Data Protection and Cybersecurity in Nigeria: Issues and Challenges'[2020] (2) Journal of Cybersecurity 56-70.

[27] Ibid.

[28] O Ajai, 'Data Protection and the Right to Privacy in Nigeria: A Comparative Analysis with the United States' [2020] (15) Journal of Comparative Law 12-28.

[29] Ibid.

[30] Ibid.

[31] O Olasoji, 'The Role of the Judiciary in Protecting Personal Data in Nigeria' [2020] (1) Journal of Judicial Studies 12-28.

knowledge or consent. This can lead to a chilling effect on free speech, as individuals may be reluctant to express themselves online for fear of being monitored or targeted. Also, another impact of AI surveillance on digital rights in Nigeria is the potential for discrimination and bias. AI-powered surveillance systems can be programmed to target specific groups or individuals based on their race, ethnicity, religion, or other characteristics. This can lead to discriminatory treatment and unequal protection under the law. For instance, AI-powered facial recognition systems have been shown to be less accurate for individuals with darker skin tones, which can lead to false positives and wrongful arrests.[32]

The use of AI-powered surveillance in Nigeria also raises concerns about data protection and privacy.[33] The government and other actors may collect and store vast amounts of personal data, including biometric data, without adequate safeguards or oversight.[34] This can lead to data breaches, identity theft, and other forms of exploitation. Furthermore, the use of AI-powered surveillance can also lead to the creation of "data profiles" that can be used to predict and influence individual behaviour.[35] The impact of AI surveillance on digital rights in Nigeria is also felt in the realm of freedom of assembly and association.[36] The use of AI-powered surveillance can make it more difficult for individuals to assemble and associate freely, as they may be subject to monitoring and tracking.[37] This can have a chilling effect on political activism and social movements, as individuals may be reluctant to participate in protests or other forms of collective action for fear of being targeted or surveyed. The deployment of AI-powered surveillance in Nigeria has significant implications for digital rights in the country. The potential for mass surveillance, discrimination, and bias, as well as the risks to data protection and privacy, all raise concerns about the impact of AI surveillance on digital rights in Nigeria. It is therefore essential that the government and other actors take steps to ensure that AI-powered surveillance is deployed in a manner that respects

[32] A Adeyeye, 'The Challenges of Implementing the Nigeria Data Protection Regulation 2019' [2020] (1) Journal of Information, Technology and Management 34-49.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] C Okoro, 'The Impact of the Nigeria Data Protection Regulation 2019 on Businesses in Nigeria' [2020] (2) Journal of Business and Economic Studies 12-25.

and protects digital rights, and that is transparent, accountable, and subject to oversight and regulation.

5. Legal and Regulatory Framework Governing AI Surveillance in Nigeria

The legal and regulatory framework governing AI surveillance in Nigeria is fragmented and inadequate. Therefore, there is no single, comprehensive law that regulates AI surveillance in Nigeria. Rather, there are various laws and regulations that touch on different aspects of AI surveillance, including data protection, privacy, and national security. Thus, section 37 of the 1999 Constitution of the Federal Republic of Nigeria guarantees the right to privacy, which includes the right to be free from unauthorized surveillance.[38] However, this right is not absolute and can be derogated from in certain circumstances, such as national security and public safety. The National Security Agencies Act, 1986 and the Terrorism (Prevention) Act, 2011 (as amended), provide some legal basis for surveillance in Nigeria. However, these laws are often vague and overly broad, allowing for abuse and arbitrary application. For instance, Section 2 of the National Security Agencies Act empowers the National Security Adviser to intercept communications and conduct surveillance on individuals suspected of posing a threat to national security.[39]

The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 is another law that touches on AI surveillance in Nigeria. Section 38 of the Act empowers law enforcement agencies to intercept electronic communications and conduct surveillance on individuals suspected of committing cybercrimes. However, the Act does not provide adequate safeguards for protecting individual rights and freedoms. The Nigerian Data Protection Regulation, 2019 is one of the recent developments that aims to regulate the processing of personal data in Nigeria.[40] The Regulation requires data controllers to obtain the consent of data subjects before processing their personal data. However, the Regulation does not specifically address AI surveillance, and it is unclear how it will be applied in practice. In terms of instances of application, AI surveillance has been used in various contexts in Nigeria, including law enforcement, national

[38] Constitution of the Federal Republic of Nigeria, 1999 (as amended).

[39] NSA, 1986.

[40] U Jerome, 'Data Privacy and Protection in Nigeria: A Review of the Legal Framework' [2020] (2) Journal of Information and Technology 21-40.

security, and private sector applications. For example, the Nigerian Police Force has used AI-powered facial recognition technology to identify and track suspects. Similarly, private companies have used AI-powered surveillance systems to monitor their premises and protect their assets.[41]

Despite these developments, there are still significant gaps in the legal and regulatory framework governing AI surveillance in Nigeria. There is a need for a comprehensive law that specifically addresses AI surveillance and provides adequate safeguards for protecting individual rights and freedoms. Additionally, there is a need for greater transparency and accountability in the deployment of AI surveillance systems in Nigeria. The legal and regulatory framework governing AI surveillance in Nigeria is fragmented and inadequate. While there are various laws and regulations that touch on different aspects of AI surveillance, there is still a need for a comprehensive law that specifically addresses AI surveillance and provides adequate safeguards for protecting individual rights and freedoms.

6. Application of AI-powered Surveillance in Nigeria

The deployment of AI-powered surveillance in Nigeria raises significant ethical concerns. One of the primary concerns is the potential for bias and discrimination in AI-powered surveillance systems.[42] These systems can be programmed to target specific groups or individuals based on their race, ethnicity, religion, or other characteristics. This can lead to discriminatory treatment and unequal protection under the law.[43] For example, AI-powered facial recognition systems have been shown to be less accurate for individuals with darker skin tones, which can lead to false positives and wrongful arrests. Another ethical concern is the potential for AI-powered surveillance to erode individual privacy and autonomy. The use of AI-powered surveillance systems can lead to a loss of anonymity and freedom of movement, as individuals may be tracked and monitored without their knowledge or consent. This can have a chilling effect on free speech and association, as individuals may be reluctant to express

[41] O Ajai, 'Data Protection and the Right to Privacy in Nigeria: A Comparative Analysis with the United States' [2020] (15) Journal of Comparative Law 12-28.

[42] C Okoro, 'The Impact of the Nigeria Data Protection Regulation 2019 on Businesses in Nigeria' [2020] (2) Journal of Business and Economic Studies 12-25.

[43] Ibid.

themselves or participate in public activities for fear of being monitored or targeted.[44]

The lack of transparency and accountability in AI-powered surveillance systems is another significant ethical concern. The use of AI-powered surveillance systems can lead to a lack of transparency and accountability, as decision-making processes are often opaque and difficult to understand. This can lead to abuse and arbitrary application of power, as individuals may be targeted or surveilled without due process or oversight. The potential for AI-powered surveillance to exacerbate existing social inequalities is another ethical concern. The use of AI-powered surveillance systems can perpetuate existing biases and inequalities, particularly in the context of law enforcement and national security. For example, AI-powered surveillance systems may be more likely to target marginalized communities or individuals, leading to further marginalization and exclusion. The deployment of AI-powered surveillance in Nigeria raises significant ethical concerns. The potential for bias and discrimination, erosion of individual privacy and autonomy, lack of transparency and accountability, and exacerbation of existing social inequalities are all pressing concerns that must be addressed. It is essential that policymakers, stakeholders, and the public engage in a nuanced and informed discussion about the ethics of AI-powered surveillance in Nigeria, and work towards developing policies and regulations that prioritize transparency, accountability, and human rights.

7. Data Protection Challenges of AI surveillance in Nigeria

The deployment of AI-powered surveillance in Nigeria poses significant data protection challenges. One of the primary concerns is the collection and processing of personal data without consent.[45] AI-powered surveillance systems can collect vast amounts of personal data, including biometric data, without the knowledge or consent of individuals.[46] For instance, the Nigerian government's use of AI-powered facial recognition technology to monitor public spaces raises concerns about the collection and processing of biometric data without consent. Another data protection challenge is the lack of transparency and accountability in AI-powered

[44] Ibid.

[45] C Okoro, 'The Impact of the Nigeria Data Protection Regulation 2019 on Businesses in Nigeria' [2020] (2) Journal of Business and Economic Studies 12-25.

[46] Ibid.

surveillance systems.[47] The use of AI-powered surveillance systems can lead to a lack of transparency and accountability, as decision-making processes are often opaque and difficult to understand. For example, the Nigerian Police Force's use of AI-powered surveillance systems to track and monitor individuals raises concerns about the lack of transparency and accountability in the decision-making process. The potential for data breaches and cyber attacks is another significant data protection challenge in AI-powered surveillance in Nigeria.[48] AI-powered surveillance systems can be vulnerable to cyber-attacks, which can result in the unauthorized access and disclosure of personal data. For instance, the hacking of the Nigerian government's database of biometric data raises concerns about the potential for data breaches and cyber-attacks. The lack of data protection regulations and enforcement mechanisms is another significant challenge in AI-powered surveillance in Nigeria. Nigeria's data protection regulations are inadequate and poorly enforced, which can lead to the abuse and exploitation of personal data. For example, the Nigerian Data Protection Regulation, 2019 is a recent development, but it is unclear how it will be enforced in practice.

The deployment of AI-powered surveillance in Nigeria poses significant data protection challenges. The collection and processing of personal data without consent, lack of transparency and accountability, potential for data breaches and cyber attacks, and lack of data protection regulations and enforcement mechanisms are all pressing concerns that must be addressed. It is essential that policymakers, stakeholders, and the public engage in a nuanced and informed discussion about data protection in AI-powered surveillance in Nigeria, and work towards developing policies and regulations that prioritize data protection and human rights.

8. International Human Rights Standards and Best Practices Related to AI-Powered Surveillance in Nigeria

The use of AI-powered surveillance in Nigeria must comply with international human rights standards, including the right to privacy, freedom of expression, and non-discrimination.[49] The United Nations

[47] C Okoro, 'The Impact of the Nigeria Data Protection Regulation 2019 on Businesses in Nigeria' [2020] (2) Journal of Business and Economic Studies 12-25.

[48]Ibid.

[49] A Adekunle, 'Data Protection and the Right to Privacy in Nigeria' [2019] (38) Nigerian Journal of Technology 123-135.

Universal Declaration of Human Rights, 1948 and the International Covenant on Civil and Political Rights, 1966 provide a framework for protecting human rights in the context of surveillance. The UN Special Rapporteur on the Right to Privacy has also emphasized the need for surveillance to be necessary, proportionate, and subject to oversight and accountability. The European Union's General Data Protection Regulation (GDPR) provides a best practice framework for data protection in the context of AI-powered surveillance.[50] The GDPR emphasizes the need for transparency, accountability, and data minimization in the processing of personal data. The GDPR also provides individuals with rights to access, rectify, and erase their personal data, as well as the right to object to processing. Nigeria can draw on the GDPR as a model for developing its own data protection regulations.[51]

The Principles on the Application of Human Rights to Communications Surveillance, 2013 provide a set of guidelines for ensuring that surveillance is conducted in a manner that respects human rights.[52] The principles emphasize the need for surveillance to be necessary, proportionate, and subject to oversight and accountability. The principles also provide guidelines for the protection of metadata, the use of encryption, and the provision of remedies for individuals whose rights have been violated. The African Union's Convention on Cyber Security and Personal Data Protection, 2014 provides a regional framework for data protection and cyber security in Africa. The Convention emphasizes the need for data protection, cyber security, and human rights to be respected in the context of AI-powered surveillance. Nigeria is a signatory to the Convention and can draw on its provisions in developing its own data protection regulations.

International human rights standards and best practices provide a framework for ensuring that AI-powered surveillance in Nigeria is conducted in a manner that respects human rights. The right to privacy, freedom of expression, and non-discrimination must be respected, and surveillance must be necessary, proportionate, and subject to oversight and accountability. Nigeria can draw on international frameworks, such as the GDPR and the African Union's Convention on Cyber Security and

[50] Ibid.

[51] Ibid.

[52] Ibid.

Personal Data Protection, in developing its own data protection regulations and ensuring that AI-powered surveillance is conducted in a manner that respects human rights. Balancing national security and digital rights in Nigeria is a complex and delicate task. On one hand, the government has a responsibility to protect its citizens from security threats, such as terrorism and cybercrime. On the other hand, the government must also ensure that it does not infringe on the digital rights of its citizens, including their right to freedom of expression, association, and privacy.

One of the major challenges in balancing national security and digital rights in Nigeria is the lack of a clear and comprehensive regulatory framework. The government has enacted several laws and regulations aimed at enhancing national security, such as the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. However, these laws and regulations are often vague and overly broad, and can be used to justify human rights violations, including the suppression of free speech and the interception of communications. Another challenge is the lack of transparency and accountability in the government's surveillance activities. The government has been criticized for its failure to provide clear information about its surveillance activities, including the types of data that are being collected, the purposes for which they are being used, and the safeguards that are in place to prevent abuse. This lack of transparency and accountability makes it difficult for citizens to hold the government accountable for any human rights violations that may occur. The government's response to security threats has also been criticized for being heavy-handed and disproportionate.[53] For example, the government has been known to shut down the internet or block social media platforms in response to security threats, which can have a disproportionate impact on citizens' ability to access information and express themselves. This approach can also drive criminal activity underground, making it more difficult to track and prosecute.

9. Conclusion/Recommendations

The deployment of AI-powered surveillance in Nigeria raises significant concerns about the balance between national security and

[53] U Jerome, 'Data Privacy and Protection in Nigeria: A Review of the Legal Framework' [2020] (2) Journal of Information and Technology 21-40.

digital rights and data protection. While AI-powered surveillance may offer benefits in terms of enhancing national security, it also poses risks to individual rights and freedoms, particularly in the context of data protection and privacy. Therefore, it is essential that policymakers, stakeholders, and the public engage in a nuanced and informed discussion about the implications of AI-powered surveillance in Nigeria.

To strike a balance between national security and digital rights and data protection, it is respectfully suggested that the Nigerian government should develop a comprehensive legal and regulatory framework that governs the deployment of AI-powered surveillance. This framework should include provisions for transparency, accountability, and oversight, as well as safeguards for protecting individual rights and freedoms. Additionally, the government should establish an independent oversight body to monitor the use of AI-powered surveillance and ensure that it is conducted in a manner that respects human rights.

Furthermore, it is recommended that the Nigerian government prioritize the development of data protection regulations that are consistent with international best practices. This should include provisions for data minimization, transparency, and accountability, as well as safeguards for protecting individual rights and freedoms. Additionally, the government should invest in public education and awareness campaigns to inform citizens about the risks and benefits of AI-powered surveillance and the importance of data protection.