journals.unizik.edu.ng/index-php/jcpl ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW

Data Protection Issues in the Management of the Bimodal Voters Accreditation System (BVAS) in Nigeria

Dr. Habiba Musa[279]

Abstract

Section 153 of the Constitution of the Federal Republic of Nigeria 1999 (the Constitution) established the Independent National Electoral Commission (INEC) to organise, undertake, and supervise elections in the country.[1]The Constitution[280] further empowered INEC to make rules for the regulation of its procedure and ensure the effective discharge of its functions. Section 148 of the Electoral Act, 2022 (the Act) also empowers INEC to issue regulations, guidelines, or manuals for the purpose of giving effect to the provisions of the Act and for its administration. Pursuant to the powers vested upon it by the Constitution and the Electoral Act, INEC issued the Regulations and Guidelines for the Conduct of Elections, 2022 (the Regulation) and the Manual for Election officials 2023 (the Manual). Section 41(1) of the Electoral Act provided that INEC shall provide suitable boxes, electronic voting machine or any other voting device for the conduct of elections. The Act[281] further stated that to vote, the presiding officer shall use the smart card reader, or any technological device prescribed by INEC for the accreditation of voters. The Bimodal Voters Accreditation System (BVAS) came into being by virtue of these provisions of the law and it is the technological device adopted by the INEC in accrediting voters in Nigeria. This paper is a discourse on the data protection issues that could arise in the utilisation and management of the BVAS.

Keywords: Data, Protection, Bimodal, Accreditation, System.

1. Introduction

The use of technology in the electoral process has become increasingly important in ensuring that elections are free, fair, and credible. Nigeria's electoral umpire, the INEC, embraced technology in order to effectively carry out its constitutional function of organising, conducting and supervising elections.[282] The technology adopted by INEC is the Bimodal Voter Accreditation System (BVAS) which was piloted in the 2021 bye-election of the Isoko South Constituency of Delta state.[283]This was followed by the deployment of the BVAS in the Anambra, Ekiti, and Osun[284] gubernatorial elections and the just concluded 2023 general elections. The BVAS is a

---

[279] **Dr. Habiba Musa** Associate Professor of Law at the Department of Public and International Law, Faculty of Law, Nasarawa State University, Keffi. Habibahmusa09@gmail.com, Habibahmusa@nsuk.edu.ng 08036164557. [1] Section 4(a) Part II of the third schedule to the Constitution.

[280] Section 160.

[281] Section 47(2).

[282] See note 1 ibid.

[283] Chidi Anselm Odinkalu, 'Let's Talk about BVAS' *The Guardian* (Lagos, 15 November 2021)<guardian.ng>accessed 26/3/2023.

[284] These elections were held on Saturday, November 6, 2021; Saturday, 18 June, 2022; and Saturday, the 16th July 2022 respectively.

system of accreditation that allows for voter authentication using fingerprint and facial recognition.[285]

While the BVAS has been praised for its effectiveness in reducing incidents of electoral fraud and ensuring that only eligible voters participate in elections, [286] there are concerns about data protection and privacy issues associated with the system. The use of biometric data in the system has raised questions about the security and privacy of personal information collected from voters. [287] Additionally, the storage and management of the data have raised concerns about the potential for misuse of personal information.

This paper explores the data protection issues associated with the management of the BVAS in Nigeria. Specifically, the paper examines the legal framework governing data protection in Nigeria, the collection and storage of personal data in the BVAS, and the potential risks associated with the use of the system. The paper also discusses the measures that can be put in place to mitigate the risks and ensure that the system is compliant with data protection laws.

To achieve these objectives, the paper is structured as follows: first, a brief overview of the BVAS is provided, followed by a discussion on the legal framework governing data protection in Nigeria. The next section examines the collection and storage of personal data in the BVAS, including the types of data collected and the measures put in place to secure the data. The potential risks associated with the use of the system are then discussed, followed by a discussion of the measures that can be put in place to mitigate these risks. The paper concludes with a summary of the key findings and recommendations for the management of the BVAS in Nigeria.

2. Overview of the Bimodal Voter Accreditation System (BVAS)

Elections are a fundamental aspect of democratic societies, and the use of technology has played a critical role in ensuring the integrity of the electoral process. One of the technologies that have been used in recent years to improve the accuracy and transparency of the voting process is the Bimodal Voter Accreditation System (BVAS).

BVAS is a technology that combines biometric and non-biometric data to verify the identities of voters during elections. This system typically involves the use of fingerprint and facial recognition technologies, as well as other data such as voter identification cards and personal information. The system compares the biometric data of voters with data stored in a central database to determine their eligibility to vote. BVAS has been implemented in several countries around the world, including India, Ghana, and Nigeria.

In India, the Election Commission of India (ECI) introduced BVAS during the 2014 general elections to ensure the accuracy and transparency of the voting process.[288] The use of BVAS was

[285] Article 2.7.1 of the Manual for Election Officials 2023.

[286] Y. Babatunde, 'Towards a Credible Electoral Process in Nigeria: The Role of Biometric Technology' [2015](3)(8)n*International Journal of Political Science and Development* 264-273.

[287] J. Abbas and M. Alotaibi, 'The Use of Biometrics in Election Management: A Review of Trends and Issues' [2018](35)(1) *Government Information Quarterly* 87-94.

[288] S. Mishraand R. Garg, 'Biometric authentication: A boon to Indian electoral process' [2016] (14)(8) International Journal of Computer Science and Information Security 146-151.

hailed as a success, with reports suggesting that it helped to reduce voter fraud and improve the credibility of the electoral process.[289]In Ghana, the Electoral Commission (EC) implemented BVAS in the 2020 general elections to verify the identities of voters and prevent voter fraud. The use of
BVAS in Ghana was also deemed successful, with reports suggesting that it helped to reduce incidents of voter fraud.[290] In Nigeria, the Independent National Electoral Commission (INEC) introduced BVAS during the 2015 general elections to improve the credibility of the electoral process.[291]

The use of technology in the electoral process has several benefits, including the automation of various aspects of the electoral process, such as voter registration, accreditation, and vote counting. This has improved the efficiency, accuracy, and transparency of the voting process, thereby enhancing the credibility of elections.[292] BVAS is an example of the use of technology in the electoral process, that provides a fast and efficient method of verifying the identities of voters and seeks to reduce election fraud. BVAS also seeks to eliminate or reduce to the barest minimum, the disadvantages of manual accreditation, which is often time-consuming and prone to errors. The automation of the accreditation process by BVAS ensures that only eligible voters are allowed to cast their votes, thereby enhancing the credibility of the electoral process.

Despite the benefits of BVAS, the use of biometric data in the system has raised concerns about data protection and privacy issues. Biometric data such as fingerprints and facial recognition are unique identifiers that can be used to track individuals, and their use raises concerns about the protection of personal information. [293] In addition, the centralisation of data in BVAS raises concerns about the security of the data. The central database contains sensitive personal information of voters, including biometric data, which could be vulnerable to hacking and other forms of cyber attacks.Unauthorised access to the database could result in identity theft, voter impersonation, and other forms of fraud.[294][295]

---

[289] A. Sharma, Fingerprint technology marks an improved voter turnout in India,(The Guardian 2014)https://www.theguardian.com/global-development/2014/may/22/fingerprint-technology-india-voter-turnout.

[290] The Ghana EC Chair, 'BVMS Performed Well in 2020 Polls' (JoyOnline December 9 2020) https://www.myjoyonline.com/news/politics/bvms-performed-well-in-2020-polls-ec-chair/.

[291] Independent National Electoral Commission (INEC). (2015). Press briefing on the performance of card readers in the 2015 presidential and national assembly elections,<https://www.inecnigeria.org/wp-content/uploads/2015/03/Press-Briefing-on-the-Performance-of-Card-Readers-in-the-2015-Presidential-andNational-Assembly-Elections.pdf>accessed 12/07/23.

[292] R. Srinivasan, 'Beyond the Valley' quoted in Stacia Brown 'Protecting the Voices beyond the Valley' https://www.the1a.orgaccessed 12/06/23.

[293] J. Mistry, 'An Evaluation of the Challenges and Opportunities of Biometric Technology in Voting Systems' [2019](4)(2) Journal of Global Security Studies, 4(2), 133-150.

[294] U. Kritzinger, M. Tshabalala, and F. Mhlanga, (2019). 'Biometric Technology in Elections: An analysis of risks and opportunities' [2019] Council for Scientific and Industrial Research (CSIR). [17]*Kamal Nath v Election Commission of India and Ors*[2019] 2 SCC 260.

[295] Polls, EC Explains Why BVMS Failed to Work in Some Constituencies (Adom Online 7th December 2020). 2020 polls: EC explains why BVMS failed to work in some constituencies. https://www.adomonline.com/2020polls-ec-

These concerns have been raised in several countries that have implemented BVAS. In India, concerns were raised about the security of the biometric data used in BVAS, and the Supreme Court of India ordered that the electoral body is 'duty bound to take all precautionary measures' to ensure the safety of data of electors.[17] In Ghana, there were concerns about the accuracy of the facial recognition technology used in BVAS, and the EC had to introduce additional measures to address the issue.[18] In Nigeria, concerns were raised about the security of the data stored in the central database, and INEC had to assure the public that the data would be protected.[296]

The concerns about data protection and privacy associated with BVAS highlight the need for the implementation of robust data protection and privacy laws in countries that use the system. These laws should ensure that the personal information of voters is protected, and that the data is not used for purposes other than those for which it was collected. In addition, the laws should ensure that the data is stored securely and that access to the data is restricted to authorised personnel only.

The use of technologies such as the BVAS, in the electoral process has several benefits, including the automation of various aspects of the electoral process, which improves the efficiency, accuracy, and transparency of the voting process. However, the use of biometric data in BVAS raises concerns about data protection and privacy issues. These concerns highlight the need for the implementation of robust data protection and privacy laws in countries that use the system, to ensure that the personal information of voters is protected, and that the data is stored securely.

3. Legal Framework for Data Protection in Nigeria

Data protection is a critical issue in Nigeria, particularly in the context of the electoral process, where sensitive personal information of citizens is collected and processed by the Independent National Electoral Commission (INEC). This section discusses the legal framework for data protection in Nigeria, focusing on the relevant provisions in the Constitution of the Federal Republic of Nigeria 1999, the Electoral Act, 2022, the Regulations and Guidelines for the Conduct of Elections, 2022, and the Manual for Election Officials 2023.

The Constitution of the Federal Republic of Nigeria 1999 is the supreme law of the land, and it contains several provisions that are relevant to data protection. Section 37 of the Constitution provides for the right to privacy, which includes the right to the privacy of correspondence, telephone conversations, and telegraphic communications. This provision guarantees the right to the protection of personal information and data by the Constitution.

In addition, Section 39 of the Constitution guarantees the right to freedom of expression and the press. This provision protects the right to access information and to express opinions on matters of public interest, including information about the electoral process. The right to access

explains-why-bvms-failed-to-work-in-someconstituencies/GhanaWeb<https://www.ghanaweb.com/GhanaHomePage/election2020/Ghana-Election-2020Electoral-Commission-explains-how-BVMS-works-1139209>accessed 17/07/2023.

[296] Nigeria Election: INEC Raises Alarm over Voter's Register Cloning (Premium Times 4th September 2018)<https://www.premiumtimesng.com/news/headlines/281779-nigeria-election-inec-raises-alarm-over-votersregister-cloning.html>accessed 17/07/2023.

information is critical to the protection of personal data, as it allows citizens to monitor the collection, processing, and use of their personal information by INEC.

The Electoral Act, 2022provides additional provisions for the protection of personal data in the electoral process. Section 150 of the Act provides that all information collected by INEC in the course of an election shall be kept confidential and shall not be disclosed to any person, except as may be required by law. This provision ensures that personal data collected by INEC is protected from unauthorised access and disclosure.

Furthermore, Section 151 of the Act provides that any person who discloses confidential information obtained during an election without lawful authority shall be liable to a fine of N10, 000,000 or imprisonment for a term of two years, or both. This provision imposes a criminal penalty on individuals who breach the confidentiality of personal data collected by INEC.

The Regulations and Guidelines for the Conduct of Elections, 2022, and the Manual for Election Officials 2023 provide detailed guidance on the collection, processing, and use of personal data in the electoral process. The Regulations and Guidelines provides that INEC shall ensure that personal data collected from voters is protected from unauthorised access, use, and disclosure. The Manual provides specific procedures for the handling of personal data, including the use of the Bimodal Voters Accreditation System (BVAS).

The Nigeria Data Protection Regulation (NDPR) was passed in 2019to regulate the processing of personal data in Nigeria. The NDPR mandates that data controllers and processors must obtain the consent of data subjects before processing their personal data and must ensure the confidentiality, integrity, and availability of the personal data they process.[297]

The enactment of the Nigeria Data Protection Act 2023(NDPA) further strengthened the robustness of the legal framework for data protection in Nigeria. Overall, the legal framework for data protection in the management of the BVAS in Nigeria comprised of the Constitution[298], the Electoral Act,[299] the Regulations and Guidelines for the Conduct of Elections,[23] the Manual for Election Officials,[24] Nigeria Data Protection Regulation,[300] and the Nigeria Data Protection Act.[26] These laws/regulations established the rights of individuals to the privacy of their personal data and provide for the protection of such data from unauthorised access, usage, and disclosure.

The legal framework further seeks for enhanced protection of personal data by mandating that data controllers and processors comply with certain principles and requirements for the processing of personal data. Therefore, the BVAS must be utilised and managed in compliance with these legal frameworks to ensure the protection of the privacy and personal data of Nigerian voters.

---

[297] Articles 2.2 and Article 3 NDPR.
[298] Constitution of the Federal Republic of Nigeria 1999.
[299] The Electoral Act 2022. [23]INEC's Regulations and Guidelines for the Conduct of Elections 2022. [24]The Manual for Election Officials 2023.
[300] Nigeria Data Protection Regulation 2019.
[26] Nigeria Data Protection act 2023.

However, there are concerns about the efficacy of the legal framework in safeguarding the data of electorates as the effective implementation and enforcement of the laws and regulations are a *sine quo non*for a data privacy and protection regime. In addition, there are concerns about the security of personal data collected by INEC, particularly in the context of the use of the BVAS. The BVAS is a biometric system that captures the fingerprints and facial features of voters for the purpose of accreditation. While the system is designed to enhance the integrity of the electoral process, there are concerns about the security of the data collected and the potential for abuse.

4. Collection and Storage of Personal Data in the BVAS

The bimodal voters accreditation system (BVAS) is an electronic voting system that employs both biometrics and smart card technology to verify the identity of voters and ensure the accuracy of their votes[301] Personal data is collected through biometric data and smart cards, and this data is stored in a secure database and on the smart card itself.[302] The biometric data refers to unique physical characteristics of individuals such as fingerprints, facial features, and iris patterns, which are captured during the voter registration process and stored in a database for use during the accreditation process.[303] The smart card is a plastic card containing an embedded microchip that stores information about the voter such as their name, address, and voter ID number, which is issued to voters during the voter registration process and used to authenticate the voter during the accreditation process. The BVAS also stores personal data on the smart card, which is encrypted to prevent unauthorized access, and the card itself is protected by a password that is known only to the voter. The smart card is designed to be tamper-proof, and any attempt to modify or copy the information on the card will render it invalid.[304]

The BVAS database is designed to store biometric data and other personal information about voters and is secured using encryption and other security measures to prevent unauthorised access.[305] The BVAS is used during the accreditation process, for the purpose of verifying and authenticating the identity of voters and ascertaining their eligibility to vote. Voter accreditation with the BVAS essentially involves the use of biometric scanners and smart card readers for the authentication of the identity of voters. During the accreditation process, the voter's biometric data is captured using a biometric scanner, and the information on the voter's smart card is read using a smart card reader. The biometric data and the information on the smart card are compared to the data stored in the database to verify the identity of the voter.[306]

---

[301] M.N. Sulaiman, Z.F.Zaaba, and R. Din, 'Bimodal Biometric Authentication System for Electronic voting'[2014] Proceedings of the 5th International Conference on Computing and Informatics IEEE 214-219.

[302] M.T. Lazarescu, M.C. Ciobotaru, and H.N. Costin, 'Towards Secure Bimodal Biometric Authentication Systems' [2015] (13) (4) Journal of Applied Logic 464-473.

[303] J. García-Baos, T. Li, andA. Potamianos, (2016). The use of biometrics in electronic voting: Handbook of electronic voting (Springer 2016) 267-302.

[304] S. Bistarelli, F. Santini, and M. Talamo, A bimodal biometric authentication system for e-voting. Electronic Voting, (2015) 9-19.

[305] M.N Sulaiman (note 27).

[306] M.T. Lazarescu (note 28).

Similarly, the use of the bimodal voter accreditation system (BVAS) in Nigeria is crucial in ensuring a transparent and fair electoral process. BVAS collects personal data of eligible voters using biometric technology, including fingerprints, facial images, and iris scans. This data is collected using electronic devices such as biometric scanners and cameras. During the voter registration process, eligible voters are required to provide their personal information, including their full name, date of birth, gender, and address. The biometric data and personal information are then stored in a central database for future use. The storage of personal data in Nigeria's BVAS is essential in preventing voter fraud and ensuring the accuracy of the electoral process.

Therefore, BVAS in Nigeria employs both biometrics and smart card technology to verify the identity of voters and ensure the accuracy of their votes. The storage of personal data in the BVAS database and on the smart card is essential in preventing voter fraud and ensuring the integrity of the electoral process. The use of electronic devices such as biometric scanners and smart card readers during the accreditation process further enhances the efficiency and transparency of the electoral process.

5. Potential Risks Associated with the Use of the BVAS

The use of biometric technology in the Bimodal Voters Accreditation System (BVAS) has revolutionised the electoral process in Nigeria by ensuring that voters' identities are authenticated in a fast and reliable manner. However, the use of this technology raises concerns about data protection and privacy, as well as storage and management of personal information. These concerns are significant given the potential risks associated with the use of biometric data and personal information.

Adebayo[307] noted that biometric data, which includes fingerprints, facial images, and iris scans, are classified as sensitive personal data under the Nigerian Data Protection Regulation 2019. As such, the collection, processing, and storage of such data must comply with the provisions of the Regulation. Adeogun et al.[308] further highlighted the risks associated with the use of biometric data, such as the possibility of identity theft, unauthorised access to personal information, and the potential for misuse of the data by electoral officials or other parties. The Nigeria Data Protection Act[309] requires organisations that collect biometric data to obtain consent from individuals, use the data only for the intended purpose, and ensure the security of the data.

In addition to the risks associated with biometric data, concerns also exist regarding the storage and management of personal information collected through the BVAS. The Independent National Electoral Commission (INEC) is responsible for ensuring that personal information is collected, processed, and stored in compliance with the NDPA and other relevant laws and regulations. The INEC's Regulations and Guidelines for the Conduct of Elections (2022) stated that personal information collected during the electoral process must be kept confidential and used only for the

[307] J. Adebayo, 'Legal Implications of Data Protection in Nigeria: A Review of the Nigerian Data Protection Regulation 2019' [2020] (11) (3). European Journal of Law and Technology, 1-14.

[308] R.O. Adeogun, I.T. Adepoju, and O. Abiona, 'Risks Associated with the Use of Biometric Technology in Election Administration in Nigeria' [2019] In Proceedings of the 2nd International Conference on E-Society, E-Education, and E-Technology IEEE 222-225.

[309] Section 24 NDPA.

intended purpose. The manual for election officials (2023) provides guidelines for the management of personal information collected through the BVAS, including the handling of complaints and requests for access to personal information.

Therefore, BVAS has enhanced the integrity of the electoral process in Nigeria by ensuring that only eligible voters are allowed to participate in elections. However, this technology presents risks related to data protection and privacy, as well as the storage and management of personal information. Adequate measures must be put in place to ensure that personal information is collected, processed, and stored in compliance with relevant laws and regulations. Additionally, Nigerian government must ensure that appropriate safeguards are in place to protect citizens' privacy and prevent misuse of personal information collected during voter registration.

6. Measures to Mitigate Risks and Ensure Compliance with Data Protection Laws The use of biometric technology in the Bimodal Voters Accreditation System (BVAS) has truly revolutionised the electoral process in Nigeria by ensuring that voters' identities are authenticated in a fast and reliable manner. However, the use of this technology raises concerns about data protection and privacy, as well as storage and management of personal information. To mitigate these risks and ensure compliance with data protection laws, several measures can be implemented, including encryption and secured storage of data, the implementation of data protection policies and procedures, and training for election officials and staff.

To mitigate the risks associated with the collection and storage of personal data, the use of encryption and secure storage methods is recommended. According to Burt,[310] data encryption is a critical measure for protecting personal data, as it involves the conversion of plain text data into cipher text using an algorithm. This process ensures that the data is secure and can only be decrypted with a specific key. In addition, secure storage methods such as firewalls and passwordprotected databases can also be implemented to prevent unauthorised access to personal information.

Implementation of data protection policies and procedures: another measure to mitigate risks is the implementation of data protection policies and procedures. This involves developing and implementing policies and procedures that outline the appropriate use and management of personal data. The policies should also specify the roles and responsibilities of individuals responsible for managing personal data.

According to Adeogun et al.[311] the development of policies and procedures for managing personal data is essential for ensuring compliance with data protection laws. The policies should outline the appropriate use and management of personal data, as well as the procedures for collecting, storing, and processing such data. Furthermore, the policies should specify the roles and responsibilities of individuals involved in the management of personal data.

Training for election officials and staff: Training for election officials and staff is another measure to mitigate risks associated with personal data collection and storage. Training can

[310] M. Burt, (2021). Understanding Encryption: A Guide to the Basics. Microsoft. Independent National Electoral Commission (2023). Manual for Election Officials.
[311] R. O. Adeogun (note 34).

increase awareness of the importance of data protection, as well as provide the necessary skills to implement data protection measures effectively.

According to the INEC's Regulations and Guidelines for the Conduct of Elections, election officials and staff involved in the management of personal data must receive training on data protection measures. The Manual for Election Officials also provides guidelines for the management of personal data, including the handling of complaints and requests for access to personal data.

The use of encryption and secure storage methods, implementation of data protection policies and procedures, and training for election officials and staff are essential measures to mitigate risks associated with the collection and storage of personal data. Nigerian government and the INEC must ensure compliance with data protection laws, as well as develop and implement appropriate measures to protect citizens' privacy and prevent misuse of personal information.

7. Recommendation

The bimodal voters accreditation system (BVAS) is indeed a great innovation that impacted greatly on the electoral process of the country. However, the use of the BVAS technology presents significant risks related to data protection and privacy, as well as storage and management of personal information.

To mitigate these risks, it is essential to implement measures such as encryption and secure storage of data, the implementation of data protection policies and procedures, and training for election officials and staff. These measures will go a long way in enhancing compliance with data protection laws and regulations and protect the privacy of citizens' personal information.

It is also recommended that the INEC should prioritise the implementation of these measures to ensure that personal information collected through the BVAS is adequately protected. The INEC should also provide training for election officials and staff on data protection laws, procedures and best practices to prevent data breaches and other privacy violations.

Furthermore, INEC should consider conducting regular audits of its data protection policies and procedures to ensure compliance with data protection laws and regulations. The INEC should also ensure that the citizens have access to information on their rights to privacy and data protection and the measures put in place to protect their personal information.

8. Conclusion

In conclusion, the bimodal voters accreditation system (BVAS) has significantly improved the electioneering process in Nigeria by ensuring the authentication of voters' identities in a reliable and efficient manner. However, these gains could be thwarted by threats that are inherent in the collection and storage of data. To maximise the advantages of the utilisation of the BVAS in the electoral process, the measures discussed in this paper should be taken into consideration in the adoption of the technological innovation.

To ensure compliance with data protection laws and regulations. The INEC should also ensure that citizens have access to information on their rights to privacy and data protection and the measures put in place to protect their personal information.