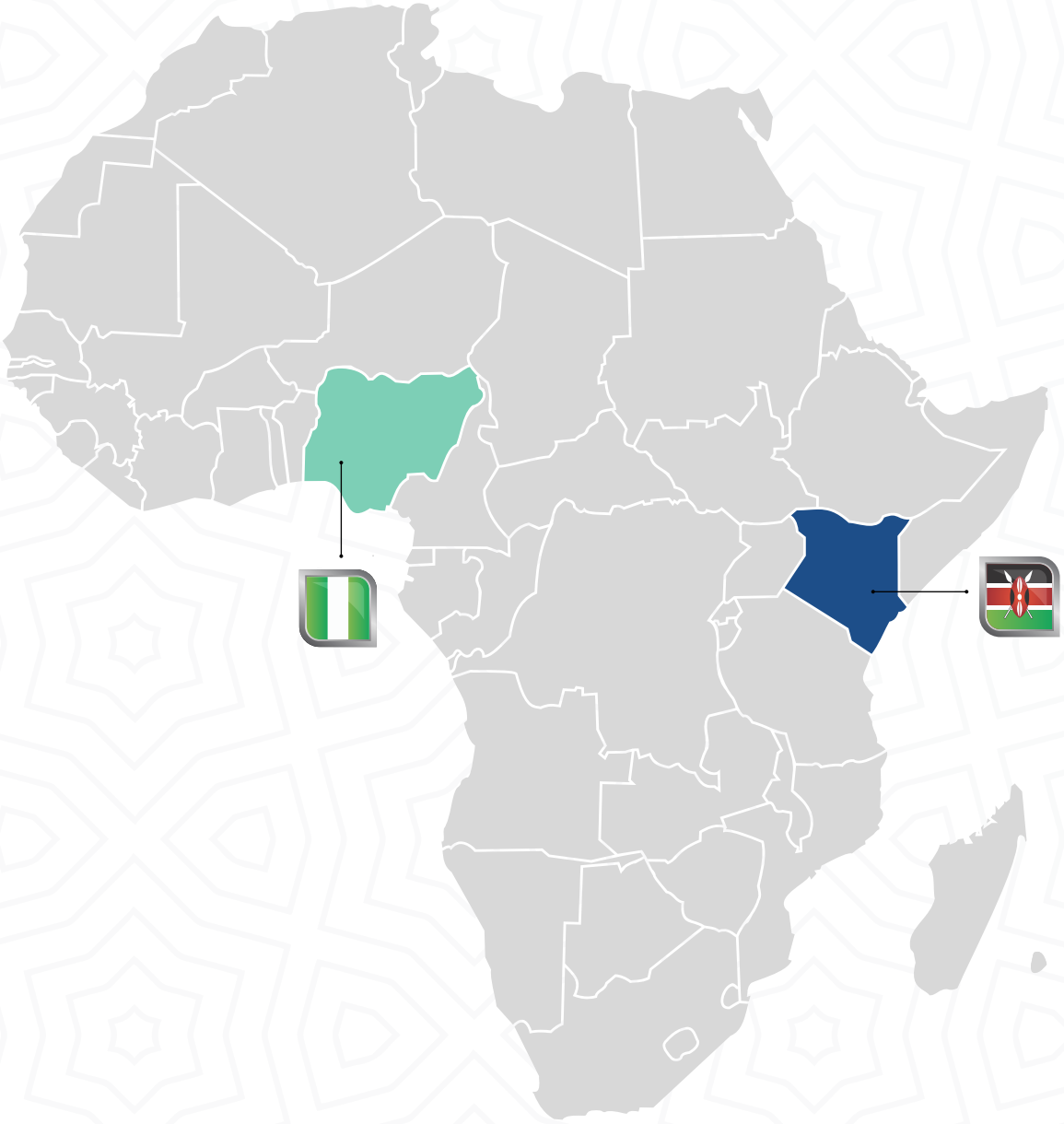
IKIGAI DATAFICATION AND DEMOCRACY FUND TECH HIVE ADVISORY

Bridging Data Governance in the Electioneering Processes of African Countries:

Nigeria and Kenya as Case Studies



Disclaimer - Usage of Publication

This research is for general educational purposes. The views, findings, and interpretations expressed herein are those of the authors. Therefore, seeking specific legal counsel before taking action based on this research is recommended. The omission of a trademark or service mark does not imply a lack of intellectual property rights associated with that name, mark, or logo.

About Ikigai Innovation Initiative

Ikigai Innovation Initiative is a non-profit organisation set up with the vision of becoming Africa's one-stop centre for technology policy. We promulgate diverse research on technology policy and legal frameworks across Africa. We also engage relevant stakeholders around the intersection of law, business and technology and advocate for better policies for the ecosystem at large. As a research and advocacy centre focused on emerging technologies, policy and research, we often collaborate with leading research institutes, academia, organisations, civil society, and individuals on policy affecting technology. We also publish and contribute to whitepapers, reports, policy briefs, infographics, guides and guidance, academic journals and publications. Our researchers work closely with government, stakeholders and ecosystem players, placing evidence and academic intuition at the heart of policymaking. We bring together the latest insights, evidence and commentary from our researchers with our one-stop-shop vision for policy by connecting policymakers, decision-makers, and practitioners with our industry-leading research. We also deliver evidence-based policy that meets society's grand challenges by advocating for social justice in the face of technology, sensitising the public to technology policies that impact their rights and lives, and promoting digital rights and digital ethics. Contact:

policy@ikigaination.org

About Tech Hive

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm that provides support services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies are altering and influencing the traditional way of doing things while acting as an innovation partner to our clients. Our experience and capability extend across Research, Policy Advisory and Intelligence, Privacy and Data Protection, Data Ethics, Cybersecurity, Start-Up Advisory, Emerging Technologies, Financial Services and Digital Health. We ensure our advice serves our clients well by having an excellent understanding of their business and the markets in which they operate through accurate policy and legislative development tracking and intelligence. Contact:

contact@techhiveadvisory.africa

Table of Contents

Introduction

For every successful democratic system, elections are the mechanism for the peaceful transfer of power and the representation of the people's will.[1] Countries like Nigeria, which has witnessed twenty-four (24) years of uninterrupted democracy since 1999, and Kenya, which has experienced democratic governance since the early 1990s, have established a cycle of regular elections. These democratic transitions represent significant milestones in their political histories, highlighting their commitment to democratic processes. However, despite these achievements, both countries face challenges that threaten the stability and effectiveness of their democracies.

In Africa, particularly in Nigeria and Kenya, challenges such as voter intimidation, electoral malpractices, and violence[2] have marred the credibility of election results. These issues have prompted the adoption of digitisation in the electioneering process to enhance the efficiency and transparency of elections as well as mitigate electoral malpractices to produce more reliable and credible electoral cycles. Nigeria's Independent National Electoral Commission (INEC) has embraced innovative technologies like the Bimodal Voter Accreditation system (BVAS) and the Results Viewing Portal (IReV),[3] while Kenya also implemented biometric technology like the Biometric voter registration system (BVRS), Electronic voter identification system (EVID), Results transmission system (RTS), Candidate Registration System (CRS) [4] for the electoral processes. However, the utilisation of these technologies raises concerns about data protection, privacy, and security, as electoral data and stakeholders' information are processed through these devices. [5] As these technologies continue to

[1] Thum Ping Tjin Bonnibel, 'Principles of Democracy: Free, Fair, Regular, and Representative Elections' (New Naratif, 12 November 2023) <https://newnaratif.com/principles-of-democracy-free-fair-regular-and-representative-elections/> accessed 15 June 2024.

[2] On bloodiest day of protests, Kenya opposition vows to keep up pressure with strikes. (n.d.). Retrieved June 20, 2024, from https://www.statesboroherald.com/local/associated-press/on-bloodiest-day-of-protests-kenya-opposition-vows-to-keep-up-pressure-with-strikes/

Bloody kenyan elections: Confronting electoral violence in 2022 - the elephant. (2021, February 12). https://www.theelephant.info/analysis/2021/02/12/bloody-elections-confronting-kenya-elections-violence-in-2022/

[3] Tobi Ayeni, et al, 'The Role of Technology in Nigeria's 2019 and 2023 General Elections', (Research Gate 2023), available at <https://www.researchgate.net/publication/376264625_The_Role_of_Technology_In_Nigeria%27s_2019_and_2023_General_Elections> accessed 10 May 2024.

[4] Japheth Ondiek, Gideon Onyango, 'African Governance in the Digital Age - Realising Digitalised Electoral Process in Africa: Public Policy Implications from Kenya's Electoral Technology Systems', (Tayarisha Working Paper Series | No:2023/005), available at <https://wiredspace.wits.ac.za/server/api/core/bitstreams/ee26f3ec-0111-4259-abbc-16436877b0bf/content> accessed 10 May 2024.

[5] Nnenna Ifeanyi-Ajufo, Dr Leena Koni Hoffmann, 'Tech Alone won't Improve Trust in Nigeria's Elections' https://www.chathamhouse.org/2023/02/tech-alone-wont-improve-trust-nigerias-elections> accessed 10 May 2024.

advance, elections have increasingly relied on data, raising concerns about misuse of personal information and potential interference with electoral results, highlighting the imperative for safeguarding the sanctity of electoral data through robust data governance frameworks.[6]

Data governance is the practice of organising and implementing policies, procedures, and standards to effectively use an organisation's structured and unstructured information assets and data.[7] It is a principled approach to managing data throughout its lifecycle, from acquisition to use to disposal, ensuring data security, privacy, accuracy, availability, and usability.[8]

In the context of electioneering processes, effective data governance can be a pivotal tool in ensuring the accuracy and reliability of electoral data, thereby maintaining the integrity of the electoral process. It promotes transparency and accountability by establishing clear guidelines for collecting, processing, and reporting electoral data. Data governance also enhances data security, safeguarding electoral data from unauthorised access or tampering.[9] Adopting data governance throughout the electioneering process, from election campaigns and voter registration to polling and result tabulation, would facilitate informed decision-making by election officials.[10] This, in turn, would foster public trust in the electoral process.

This research explores the data governance in electoral processes in Nigeria and Kenya, drawing insights from existing literature, past experiences, and case studies. This research examines data governance in the context of electioneering processes in Nigeria and Kenya. The research aims to distil broad recommendations and best practices tailored to these countries' electioneering process. Ultimately, this will contribute to enhancing democratic practices and safeguarding electoral integrity across the continent.

[6] Ekdale, B., & Tully, M. (2020, January 9). How the nigerian and kenyan media handled cambridge analytica. The Conversation. http://theconversation.com/how-the-nigerian-and-kenyan-media-handled-cambridge-analytica-128473
Foundation, B. A., Thomson Reuters. (2023, February 24). FEATURE-ID of 93 million Nigerians at risk in landmark election. Reuters. https://www.reuters.com/article/markets/commodities/feature-id-of-93-million-nigerians-at-risk-in-landmark-election-id USL8N35360C/
Sibe, R. T., & Kaunert, C. (2023). Technology, cyber security and the 2023 elections in Nigeria: Prospects, challenges and opportunities. Journal of African Elections, 22(2). https://doi.org/10.20940/JAE/2023/v22i2a4

[7] 'Data Governance Explained' (AltexSoft) <https://www.altexsoft.com/blog/data-governance/> accessed 15 June 2024.

[8] Vijay Kanade, 'What is Data Governance?: Definition, Importance and Best Practices', available at; <https://www.spiceworks.com/tech/big-data/articles/what-is-data-governance-definition-importance-and-best-practices/> accessed 9 May 2024.

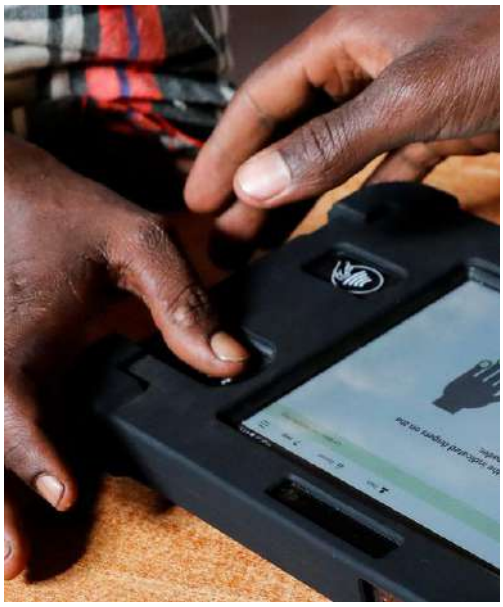
[9] Handbook for the Observation of Election Administration. Warsaw, Poland: Author. OSCE Office for Democratic Institutions and Human Rights (ODIHR). (2023).accessed 20 June 2024

[10] Department of Information & Communications Technology. (2023). Data Governance & Data Protection Policy, Version 5.0.

Understanding the Impact of the Deployment of Technology and Innovation in Elections

Over the years, many countries have continued to embrace technology to improve governmental efficiency, and that has extended to the electoral process.[11] With the introduction of technology, common issues associated with traditional voting systems have been minimised[12]. In the early 1880s, elections were conducted using the "viva voce" system, which allowed voters to vote orally by saying "yea" or "nay."[13] Apart from this, there have been other open voting systems which have occasioned various dangers, such as a consistent increase in election violence, vote manipulation, and even ballot snatching.[14] With the introduction of technology, there has been a surge in more data-driven elections, which has helped electoral commissions keep adequate voters' records, fight electoral malpractices, and ensure accuracy in result collation.[15]

However, electoral processes and procedures have continued to develop and evolve. Nigeria has experienced different phases in developing its electoral system and has embraced technology. In the 1993 elections, Nigeria adopted the "Option A4" model, an open voting system that required voters to queue behind their preferred candidates.[16] The initial phase of data-driven elections was manual, as voters were issued paper voter identity cards. This phase primarily involved personally identifiable information. With time, biometric-based voter identity cards were introduced. Card readers were introduced to verify voters and ensure that only registered voters could vote during elections to ensure the system's transparency further.



The Independent National Electoral Commission (INEC) began introducing technological solutions in the electoral system in 2002 with the Optical Mark Recognition (OMR) technology, which was used for voter registration for the 2023 elections. [17] During the 2007 elections, the electronic voter register, electronic voting machines, electronic voter authentication, and electronic transmission of results were introduced. [18] These electronic systems used and collected data such as biographical data, thumbprints, and the photographs of voters. In 2011, the Direct Data Capture Machines (DDCMs) were launched to capture the biodata, photographs, and all 10 fingerprints of voters. The voters' register was

[11] Dad, Nighat, and Shmyla Khan. "Reconstructing Elections in a Digital World." South African Journal of International Affairs, vol. 30, no. 3, July 2023, pp. 473–96. DOI.org (Crossref), https://doi.org/10.1080/10220461.2023.2265886.
[12] Professor Mahmood Yabkubu, 'Technological Innovation as Antidote to Election Rigging' (2021) accessed 20 June 2024
[13] 'Election Technology Through the Years - The Council of State Governments' (8 November 2023) <https://www.csg.org/2023/11/08/election-technology-through-the-years/> accessed 13 May 2024
[14] Bart Engelen, 'Against the Secret Ballot: Toward a New Proposal for Open Voting', (ResearchGate, 2013) accessed June 19, 2024
[15] Professor Mahmood Yabkubu, 'Technological Innovation as Antidote to Election Rigging' (2021) accessed 20 June 2024
[16] Let's Return to Option A4 Electoral System - Daily Trust' (https://dailytrust.com/, 6 April 2019) <https://dailytrust.com/lets-return-to-option-a4-electoral-system/> accessed 13 May 2024
[17] International Institute for Democracy and Electoral Assistance, 'Introducing BiometricTechnology in Elections' (2017)
[18] Ibid

produced with this system, and due to its reliability, it was utilised for the general elections in 2011 and 2015.[19] The Permanent Voter Cards (PVCs) and Smart Card Readers (SCRs) were used to identify and authenticate voters during the 2015 general elections.[20]

The last two elections in Nigeria witnessed a spike in the introduction of technology in the election system. In the 2019 election, the Collation Support and Results Verification System (CSRVS), Smart Card Reader registrations and white-listing, and real-time tracking of election materials were introduced to ensure the verification of registered voters, the collation of results, and the transparency and cooperation of all stakeholders during the election.[21] The 2023 general elections witnessed the introduction of an entirely new set of technologies that differed from all previous technologies, such as the INEC Voter Enrolment Device (IVED), Bimodal Voter Accreditation System (BVAS), and INEC Results Viewing (IReV), which facilitated registration, accreditation, and collation of results during the election. [22]

In Kenya, technological advancements have played a crucial role in enhancing electoral processes. Kenya began infusing technology in its electoral process following the recommendations of the Report of the Independent Review Commission on the General Elections held in Kenya in 2007. The 2007 election in Kenya was rigged with structural issues that led to a series of violence that caused the loss of lives and properties. The Independent Review Commission (IRC) recommended that the use of technology will drastically minimise such violence during elections, and that led to a technological reform in Kenya's electoral system.[23] Following the 2007 humanitarian crisis, the Independent Electoral and Boundaries Commission (IEBC) introduced various technologies in the 2013 general elections, including Biometric Voter Registration (BVR), Electronic Voter Identification Devices (EVID), and a Results Transmission System (RTS),[24] aiming to address issues like ballot stuffing and improve overall poll management. Despite challenges like a compressed voter registration timeline and procurement issues, the 2013 elections marked significant progress compared to previous ones, reducing irregularities and enhancing transparency.[25]

Embracing technology, such as biometric technology, in Kenya's election increased the number of voters from 14.3 million in 2013 to 19.6 million in 2017 and 22.1 million in 2022. [26] During the 2017 election cycle, the IEBC introduced the Kenya Integrated Management System (KIEMS), which it hoped would resolve the credibility issues that had previously plagued electoral processes.[27] In the 2022 general election, the IEBC further leveraged technology by digitally publishing handwritten result forms from

[19] Ibid
[20] International Institute for Democracy and Electoral Assistance, 'Introducing BiometricTechnology in Elections' (2017)
[21] Tobi Ayeni, Atachin James, 'The Role of Technology In Nigeria's 2019 and 2023 General Elections' (December, 2023)
[22] Ibid
[23] 'Kenya's Technology Evolved. Its Political Problems Stayed the Same.' (MIT Technology Review) <https://www.technologyreview.com/2018/08/22/140633/kenyas-technology-evolved-its-political-problems-stayed-the-same/> accessed 16 May 2024
[24] Ayesha Chugh and Katherine Krueger, 'The Role of Technology in the Outcome of the Kenyan General Election' <https://www.aceproject.org/today/feature-articles/the-role-of-technology-in-the-outcome-of-the/discussion_reply_form> accessed 12 May 2024.
[25] ibid
[26] 'Kenya's Election Uses High-Tech "Checks"' (Voice of America, 4 August 2022) <https://www.voaafrica.com/a/kenya-s-election-uses-high-tech-checks-/6686592.html> accessed 13 May 2024
[27] Sosi J, 'Things Kenyans Need to Know about the New IEBC KIEMS Kit before and after They Vote' (The Standard) <https://www.standardmedia.co.ke/ureport/article/2001250595/what-kenyans-need-to-know-about-the-iebc-kiems-kit-and-provisional-election-results-transmission> accessed 14 May 2024

over 46,000 polling stations, facilitating citizen-driven result tabulation and ensuring prompt release of raw local tallies after voting closed.[28] This combined approach of paper ballots and digital transparency notably contributed to a peaceful electoral process compared to other elections.

Data collection has always been a key aspect of every manual or technology-driven election. However, the advent of technology has significantly amplified the scale and accessibility of the data collected during elections, underscoring the magnitude of the issue. Data-driven elections have exacerbated data-driven campaigns, increased surveillance, voter profiling, electoral manipulation, subterfuge,[29] foreign interference, targeted campaigns, and voter manipulation.[30] The lack of transparency in the operations of electoral commissions is evident through the absence of mechanisms for voters to seek redress and mitigate risks efficiently. Notably, there is no visible mechanism for redress on their platforms, nor is there a privacy notice on both INEC and IEBC's sites or for elections. Additionally, there are no publicly declared security standards. This lack of transparency raises significant concerns about the integrity and accountability of the electoral process.

Embracing technology in elections has been justified by its prospects to encourage better voter participation, reduce political apathy, check rigging, and promote the credibility and transparency of elections.[31] Nevertheless, this system has been accompanied by cybersecurity threats and data protection violations.[32] For instance, in Nigeria, there is no adequate data protection mechanism in the registration process, as the voters' register, which contains all the details of voters, is publicly displayed during elections. Also, the PVCs are grossly exposed, as uncollected PVCs are often exposed to unauthorised individuals.[33] It also appears that political parties have access to voter's information, which they use for lobbying.[34] With the PVC system and the collection of biometric data, there have been concerns about the government using that volume of information as a tool of mass surveillance, which can be used to target activists and campaigners during protests following an unpopular election result. [35]

---

[28] Andrew Crawford, Paper Ballots with Digital Transparency: Kenya's Pioneering Election, (GIGA Focus Africa 2022 Number 7, ISSN: 1862-3603) <https://www.giga-hamburg.de/en/publications/giga-focus/paper-ballots-with-digital-transparency-kenya-s-pioneering-election> accessed 15 May 2024

[29] Kefford, Glenn, et al. "Data-Driven Campaigning and Democratic Disruption: Evidence from Six Advanced Democracies." 30 Party Politics, vol. 29, no. 3, May 2023, pp. 448–62. DOI.org (Crossref), https://doi.org/10.1177/13540688221084039.

[30] Unit, The Constitution. "Data-Driven Campaigning: The Shape and Perils of the Modern Election Campaign." The Constitution Unit Blog, 22 Jan. 2024, https://constitution-unit.com/2024/01/22/data-driven-campaigning-the-shape-and-perils-of-the-modern-election-campaign/.

[31] Osita Agbu, 'Election Rigging and the Use of Technology: The Smart Card Reader as the Joker in Nigeria's 2015 Presidential Election', <https://www.eisa.org/storage/2023/05/2016-journal-of-african-elections-v15n2-election-rigging-use-technology-smart-card-reader-joker-nigerias-2015-presidential-election-eisa.pdf> accessed 23 June 2024.

[32] Sibe, R. T., & Kaunert, C. (2023). Technology, cyber security and the 2023 elections in Nigeria: Prospects, challenges and opportunities. Journal of African Elections, 22(2). https://doi.org/10.20940/JAE/2023/v22i2a4

[33] Odunsi, W. (2022, August 15). INEC displays voters' register in Lagos. Daily Post Nigeria. https://dailypost.ng/2022/08/15/inec-displays-voters-register-in-lagos/

[34] AI and african elections: Efficiency gains hinge on trust and proper governance | democracy in africa. (2024, June 19). https://democracyinafrica.org/ai-and-african-elections-efficiency-gains-hinge-on-trust-and-proper-governance/

[35] Foundation TR, 'Data of 93 Million Nigerian Voters at Risk as Election Looms' (The National, 24 February 2023) <https://www.thenationalnews.com/world/africa/2023/02/24/data-of-93-million-nigerian-voters-at-risk-as-election-looms/> accessed 13 May 2024

Picture credit: Channelstv.com

Likewise, there have been claims of invasion of privacy. INEC claims that it maintains confidentiality, but voters' experiences prove otherwise, as there have been several reports of invasion of privacy by political parties.[36] Voters have reported instances where agents of political parties called them and rolled out their personal information as it appears on their voter's card, as well as stated the voter's polling unit.[37] The implications of this go as far as identity theft, unauthorised surveillance, and even stalking. There are also concerns that the efficacy of the tech-backed systems was not properly tested before deployment,[38] which allows for inaccuracies and possible cyberattacks.

With a surge in the use of technology in almost all aspects of the electoral process, there are real possibilities of a cybersecurity attack. All the technologies deployed by INEC are prone to both local and foreign interference and cyber threats.[39] Kenya also witnessed a sharp increase in the reports of hacking attempts and disinformation campaigns on social media.[40] Also, Kenya's election has recorded a surge in the access and use of personal data for political campaigns, as political parties used bulk SMS texting to target certain constituents to solicit votes. There are also reports of microtargeting through social media platforms by Cambridge Analytica.[41] To regulate the use of targeted SMS during the elections, the Guideline on Bulk Messaging and Social Media Communications was published to address hate speech and the incitement of violence. However, it does not address the issue of consent and the use of data.[42]

Furthermore, Nigeria currently practises the adult suffrage system, which presumes that only adults are allowed to vote. However, there are records of children voting during elections as registered voters.[43] This implies that INEC collects children's data, but there is no proof of parental consent in collecting these data. The fact that children can vote during elections also suggests that there are no age-verification mechanisms embedded in the registration of voters and data collection. This system violates the provisions of the Nigeria Data Protection Act on obtaining valid consent and implementing age-verification mechanisms. Children are left more vulnerable to privacy breaches and cyber threats without appropriate safeguards. Unfortunately, children are less likely to seek redress or lodge complaints when a data breach occurs.

[36] Foundation BA Thomson Reuters, 'FEATURE-ID of 93 Million Nigerians at Risk in Landmark Election' Reuters (24 February 2023) <https://www.reuters.com/article/idUSL8N35360C/> accessed 13 May 2024
[37] Ibid
[38] Ibid
[39] Ibid
[40] 'Cyber Threats in Elections. As Nigerians Decide in the Coming Elections.' <https://www.linkedin.com/pulse/cyber-threats-elections-nigerians-decides> accessed 14 May 2024
[41] 'Further Questions on Cambridge Analytica's Involvement in the 2017 Kenyan Elections and Privacy International's Investigations | Privacy International' <http://privacyinternational.org/long-read/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy> accessed 16 May 2024
[42] 'In Kenya's 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand' <https://carnegieendowment.org/research/2022/08/in-kenyas-2022-elections-technology-and-data-protection-must-go-hand-in-hand?lang=en> accessed 16 May 2024
[43] BusinessDay. "Nigeria in the Throes of Underage Voting." Businessday NG, 19 Mar. 2023, https://businessday.ng/analysis/article/nigeria-in-the-throes-of-underage-voting/.

Effects of Limited Data Governance Frameworks and Practices: Kenya and Nigeria as Case Studies

Overview of the Kenyan and Nigerian Data Governance Landscape

The African data governance landscape, particularly data protection, has evolved in the past few years, with more countries adopting data protection legislation and establishing authorities to enforce them.[44] Kenya and Nigeria are among the countries that have data protection laws and authorities that enforce them.[45] While Kenya has had a data protection law since 2019, Nigeria only enacted a comprehensive data protection law in 2023. [46] Before then, the regulatory framework for data protection in Nigeria was the Nigeria Data Protection Regulation (NDPR) and the NDPR Implementation Framework.[47] After the Act came into effect, the regulatory framework expanded beyond the regulations, officially creating a supervisory authority, the Nigerian Data Protection Commission (NDPC), to enforce the law. The Data Protection Act of 2019 serves as Kenya's comprehensive framework for data protection, and the implementing regulations issued by the data protection authority aid data controllers with compliance. [48] These laws enhance privacy and data protection, ensuring that personal data is handled in compliance with legal standards. In the context of elections, these frameworks impose obligations on data controllers (the electoral agencies) to ensure the protection and security of the data they process during elections, including voter registration, data storage, and result transmission.

The data protection authorities (DPAs) play a crucial role in effective data governance during elections through appropriate regulation. For example, some countries, like Kenya, Senegal[49] and South Africa, have published specific guidelines on data protection during elections. Several factors, including threats to the privacy and security of individuals in past elections, have triggered regulatory responses from these DPAs. South Africa's recent guidance note on the processing of personal data during elections[50] followed the security compromise with the country's Independent Electoral Commission (IEC)[51] and concerns about misinformation and disinformation during elections. The incident involved the unlawful disclosure of the candidate lists of two political parties. Although the regulator launched investigations into the breach as soon as it received the data breach notification, it was necessary to publish a guidance note on elections to safeguard the privacy rights of voters and curtail future incidents.

---

[44] Oloyede R and Tsebee D, 'Roundup on Data Protection in Africa - 2023' <https://www.techhiveadvisory.africa/report/roundup-on-data-protection-in-africa—-2023> accessed 8 May 2024.

[45] Ibid.

[46] 'Resources - NDPC' <https://ndpc.gov.ng/Home/Resources> accessed 9 May 2024.

47 Ibid.

[48] 'Regulatory Framework - Office of the Data Protection Commissioner (ODPC)' (21 March 2024) <https://www.odpc.go.ke/regulatory-framework/> accessed 9 May 2024.

[49] 'Communiqué Sur Le Mini-Guide Sur Le Traitement Des Données à Caractère Personnel Dans Le Cadre Du Système de Parrainage Pour Les Élections Au Sénégal | CDP'

[50] Information Regulators Guidance Note on Processing Personal Information of Voters and the Countering of Misinformation and Disinformation During Elections, available at <https://inforegulator.org.za/wp-content/uploads/2020/07/FINAL-GUIDANCE-NOTE-ON-THE-PROCESSING-OF-PERSONAL-INFORMATION-OF-VOTERS-AND-THE-COUNTERING-OF-MISINFORMATION-AND-DISINFORMATION-DURING-ELECTIONS.pdf.> accessed May 15, 2024.

[51] Information Regulator, 'Media Statement: Information Regulator Confirms Receipt of Notifications of Security Compromise from IEC' (March 11, 2024) available at <https://inforegulator.org.za/wp-content/uploads/2020/07/Media-Statement-on-the-IEC-Security-Compromise.pdf> accessed May 16, 2024.

The spread of undesirable content during elections is also an issue that DPAs have tried to curb, even collaborating with communication authorities to regulate it. There have been situations where people have been profiled based on their political data and targeted messages sent to them to change their views. This was prevalent during the 2017 general elections in Kenya, where there was widespread dissemination of fake news and unsolicited messages from political parties. Following these unfortunate incidents, the Communications Authority of Kenya, in collaboration with the National Cohesion and Integration Commission (NCIC), developed guidelines in July 2017 to regulate and prevent the transmission of undesirable political content via SMS and social media platforms.[52] The Office of the Data Protection Commissioner also developed a Guidance Note on Processing Personal Data for Electoral Purposes in 2023 that sought to assist data controllers and data processors dealing with voter personal data, including sensitive personal data, to comply with the Data Protection Act.

Data governance is just as crucial in electoral processes as it is in business relationships. The framework ensures that data processing activities in each stage of the data lifecycle are responsibly done in a way that maximises benefits for relevant stakeholders while complying with relevant ethical and legal requirements.[53] The legal frameworks in Kenya and Nigeria establish regulatory agencies and laws that regulate electoral processes, ensuring the smooth conduct of elections. The Independent National Electoral Commission (INEC) oversees Nigeria's electoral process, ensuring that data handling complies with the regulatory frameworks for data governance, including the electoral laws.[54] INEC's framework includes voter registration, data storage, and handling protocols to prevent unauthorised access and ensure the accuracy and security of electoral data.[55] The Nigerian Electoral Act provides guidelines for electoral processes, including voter registration and election conduct.[56] Other data governance laws applying generally and specifically include the Nigerian Constitution, the Cybercrimes Act 2024 (as amended), the Credit Reporting Act 2017, the Freedom of Information Act 2015, the National Identity Management Commission Act (NIMC) 2007, the Nigerian Commissions Act (NCA) 2003, and the Child Rights Act 2003, among others. These laws provide general guidelines on the management and protection of different categories of data held by the agencies.

[52] Dokeza - Making Our Own Laws' (DOKEZA) <https://info.mzalendo.com/> accessed 16 May 2024.
[53] Eke D and others, (Centre for the Study of African Economies (CSEA) :2022) 'Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs'. Available at <https://cseaafrica.org/wp-content/uploads/2022/08/DG-Institutional-gaps-and-capacity-needs-Whitepaper.pdf> accessed May 8, 2024.
[54] 'INEC Nigeria – Independent National Electoral Commission' <https://www.inecnigeria.org/> accessed 9 May 2024.
[55] Ibid.
[56] Nigerian Electoral Act 2022 , available at <https://placng.org/i/wp-content/uploads/2022/02/Electoral-Act-2022.pdf > accessed May 9, 2024.

Similarly, the Independent Electoral and Boundaries Commission (IEBC) primarily oversees data governance in Kenya's election systems and operates under regulations set by the IEBC Act.[57] Other key regulatory frameworks for data governance include the 2010 Constitution, the Kenya Information and Communication Act,[58] which outlines the rules for electronic data management and the Election Act,[59] which details the processes and requirements for elections.

Although regulatory frameworks are in place, doubts have arisen regarding their sufficiency, implementation, and efficacy across multiple elections. Privacy and security concerns stemming from inadequate data governance have manifested in historical electoral processes. This deficiency in data governance has precipitated unfavourable outcomes in previous Kenyan and Nigerian elections, underscoring the imperative for robust data governance frameworks to be implemented throughout the electoral cycle. Some of these issues will be discussed in the case studies below:

Data Governance and Elections in Kenya and Nigeria

The introduction of technology into electoral processes was initially set as a solution to a myriad of issues associated with traditional voting methods, such as paper ballots and manual counting, promising efficiency, accuracy, and accessibility for voters. [60] However, these technologies have also created concerns about the abuse of digital rights. The lack of public information about whether a Human Rights Impact Assessment (HRIA) or Data Protection Impact Assessment (DPIA) was conducted before deploying election technologies raises significant concerns. Case studies have highlighted a troubling trend wherein the very technology meant to enhance democracy has inadvertently created new vulnerabilities and risks. Instances of voter privacy concerns in electoral processes include the collection and processing of biometric data and digital identity (ID), which may exacerbate exclusion and inequality among marginalised groups; the disclosure of voters' personal data violating data protection principles; gaps in enforcing data subjects' rights regarding their voting data; the absence of privacy notices on electoral websites; misuse of personal information for digital campaigning purposes; and documented privacy issues in other African countries like Kenya and Nigeria.[61]

[57] Independent Electoral and Boundaries Commission Act 2011, available at <https://www.iebc.or.ke/uploads/resources/8Z5fmROhVD.pdf> accessed May 9, 2024.
[58] Kenya Information and Communication Act (Revised 2011) available at <https://infotradekenya.go.ke/media/Kenya%20Information%20Communications%20ACT.pdf> accessed May 9, 2024.
[59] Elections Act 2011, available <https://www.iebc.or.ke/uploads/resources/kql5cmgeyB.pdf> accessed May 9, 2024.
[60] 'The Evolution of Voting Technology: From Paper to Electronic Voting Solutions' (ElectionBuddy) <https://electionbuddy.com/blog/2023/08/29/the-evolution-of-voting-technology-from-paper-to-electronic-voting-solutions/> accessed 23 June 2024.
[61] Ikigaination.Org, 'Data Protection and Elections: Is Nigeria's democracy being undermined?' (27 February 2023) https://ikigaination.org/data-protection-and-elections-is-nigerias-democracy-being-undermined/ accessed 9 July 2024.

Moreover, the rapid pace of technological advancement often outpaces regulatory frameworks, leaving gaps in oversight and accountability. While technology has undoubtedly transformed electoral processes, it has also introduced a host of new challenges that must be addressed to ensure the integrity and fairness of democratic systems.[62] Thus, solving the challenges associated with digitised elections necessitates a meticulous step-by-step approach, beginning with a comprehensive review of data governance practices.

Data collection and management

In any electoral process, the collection and management of data during elections are central to ensuring the integrity and fairness of the electoral process. In Nigeria, for instance, the process of collecting voter data involves making it publicly available for verification,[63] violating principles of data protection and international best practices for data protection and security. Additionally, the absence of clear procedures for managing data subject rights exacerbates these issues, leaving citizens without recourse.[64]

In many jurisdictions, voting is regarded as a fundamental civil duty, yet there is typically no mandatory legal requirement for universal voting participation. Instead, voting is upheld as a right that citizens are encouraged to exercise as an integral part of democratic participation, potentially due to operational challenges in enforcement.[65] As a result, the emphasis is placed on promoting voter engagement and turnout through education, awareness campaigns, and fostering a culture of democratic participation rather than enforcing mandatory voting laws.

The lack of clear procedures for data subjects to exercise their rights and the absence of transparent processes by electoral bodies further undermine individuals' rights to privacy and protection. This lack of clarity also hampers their ability to seek redress, should they choose to do so.

Data security and privacy

Data security and privacy have emerged as critical issues in recent elections in Nigeria and Kenya, given the significant implications for individual rights and the integrity of the electoral process. Reports indicating Nigeria's weak cybersecurity infrastructure and attempted hacking of INEC's computer systems underscore the urgency of mapping cybersecurity threats and coordinating efforts to fortify electoral data security.[66] Additionally, the absence of privacy notices on INEC's and IEBC's websites and the lack of transparency regarding data protection measures further exacerbate these concerns, casting doubt on the integrity of electoral data management practices.[67]

---

[62] ACE Project, 'Elections and technology' (no date) https://aceproject.org/ace-en/topics/et/explore_topic_new accessed 1 July 2024

[63] Chinedu C, 'INEC Displays Preliminary Voter's Register in Rivers' Daily Post Nigeria (16 August 2022) https://dailypost.ng/2022/08/16/inec-displays-preliminary-voters-register-in-rivers/ accessed 9 July 2024.

[64] Eke D and others, 'Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns' (2022)

[65] 11 Journal of Responsible Technology 100039 https://doi.org/10.1016/j.jrt.2022.100039 accessed 9 June 2024.
Chapter IV or the 1999 Nigerian Constitution

[66] Ufuoma V, 'Hackers Attacked Our Result Portal during Ekiti, Osun Elections - INEC' The ICIR (9 September 2022) https://www.icirnigeria.org/hackers-attacked-our-result-portal-during-ekiti-osun-elections-inec/ accessed 9 July 2024.

[67] Article 2.5 of the Nigerian Data Protection Regulation https://inecnigeria.org/

Both Nigeria and Kenya have witnessed instances of digital campaigning and the commodification of voters' data, where political parties and campaign groups exploit personal information for targeted messaging, often without a lawful basis. In Kenya's 2017 election, voters were involuntarily enrolled in political parties through the eCitizen platform, leading to microtargeting and receiving unwanted messages from election candidates.[68] Additionally, there were instances of hackers and disinformation specialists sending bulk messages to create the illusion that they were from specific thought leaders or opposing parties in the country.[69] In Nigeria, there have also been violations of citizens' data protection rights by political entities through unsolicited messaging, with instances of parties obtaining voter data from polling units, sending bulk messages directing voters to websites for monetary incentives in exchange for their data.[70]

Kenya's 2017 elections highlighted the critical role of data governance in ensuring electoral integrity, particularly concerning the management of electronic voting systems. The irregularities in data transmission and the mishandling of electoral data, which led to the nullification of the presidential election results, underscored the vulnerabilities in the electronic systems used by the IEBC. It reinforced the importance of adhering to constitutional and legal frameworks in electoral practices, particularly the transparent and verifiable management of electoral data and the privacy of voters. This could be attributed to the insufficient regulatory framework for data governance at the time, particularly data protection and a lack of clear policies to guide the integrity of the technological systems deployed for the elections. Similarly, inadequate data governance significantly impacted the 2007 Nigerian general elections, manifesting through irregular voter registers, late or missing electoral materials, and unsecured ballot processes.[71] This lack of robust data management and security practices led to widespread allegations of electoral fraud, including ballot stuffing and falsification of vote counts.[72] The immediate outcome was a deeply flawed election that lacked credibility both domestically and internationally, leading to a questioning of democratic norms in Nigeria.

Data stewardship and ownership

Data stewardship and ownership are crucial components of data governance, particularly in the context of elections. Determining who owns electoral data and who is accountable for its stewardship can be contentious. Various stakeholders, including government agencies, political parties, and private companies (e.g., those providing digital voting platforms), often have differing views on data ownership.

Concerns also arise regarding the technologies used for data collection, particularly when these technologies are developed outside of Africa and used to gather large sets of biometric and sensitive

[68] Tactical Tech, 'Kenya: Data and Digital Election Campaigning' https://ourdataourselves.tacticaltech.org/posts/overview-kenya/ accessed 14 May 2024.
[69] Ibid
[70] Adanikin O, '2019 Election: How APC May Have Benefited from NCC, INEC Breach of Voters' Privacy' The ICIR (1 February 2019) https://www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/ accessed 9 June 2024.
Ojukwu D, 'CONFIRMED: APC Crediting Voters With N10,000 Online in Exchange for Their Data' Foundation For Investigative Journalism (10 February 2023) https://fij.ng/article/confirmed-apc-crediting-voters-with-n10000-online-in-exchange-for-their-data/ accessed 9 June 2024.
[71] Adebayo PF and Shola JO, (n 14).
[72] Osita Agbu, 'Impact of Elections on Governance: Lessons Learned' (2016: Research Gate) available at <https://www.researchgate.net/publication/321992590_Impact_of_the_Elections_on_Governance_Lessons_Learned> accessed May 9, 2024.

data, considering the possible implication of foreign actors interfering in local political campaigns and the potential misuse of personal data for political gain.[73] The lack of publicly published assessments, such as Data Protection Impact Assessments (DPIAs) or Human Rights Impact Assessments (HRIAs), creates a significant problem. This absence of such transparency raises concerns about whether voter privacy and data security are being adequately considered. While data localisation might not automatically ensure data protection, the absence of appropriate safeguards and thorough assessments before implementing such technologies poses a threat to the protection of electoral data and undermines public trust in the electoral system.[74]

For example, IEBC's failure to conduct a Data Protection Impact Assessment (DPIA) and to publish a privacy notice on its platform were notable gaps during Kenya's elections.[75] Additionally, the 2022 KPMG pre-election audit report on the voter register highlighted numerous deficiencies in data management,[76] including instances of illegal and duplicate registrations, as well as registrations of deceased individuals based on the data of other voters. Security vulnerabilities within the system were also identified, along with instances of unauthorised transfers of voters from their designated polling centres to other locations.[77] The report made recommendations, which the IEBC reported had been implemented before the elections in August 2022. Additional security measures prior to the election came from some platform owners, like TikTok, which launched the Kenyan general election guide in-app as part of its peace and safety initiative aimed at curbing misinformation during elections.[78] These efforts, coupled with the recurring issues, have necessitated the need for more robust frameworks for data governance during elections.

These case studies from Nigeria and Kenya underscore the critical importance of data governance in ensuring the integrity of electoral processes. They reveal how vulnerabilities in data handling and technology can significantly impact election outcomes and the rights of voters, leading to disputes and undermining public trust in the democratic process.

[73] Ekdale, B., & Tully, M. (2020, January 9). How the nigerian and kenyan media handled cambridge analytica. The Conversation. http://theconversation.com/how-the-nigerian-and-kenyan-media-handled-cambridge-analytica-128473
Ogbonna, Anthony. "INEC's BVAS Voting Technology: The Loopholes." Techuncode, 11 Nov. 2021, <https://techuncode.com/bvas-voting-technology-the-loopholes/.> accessed 14 May 2024.
[74] Sibe, R. T., & Kaunert, C. (2023). Technology, cyber security and the 2023 elections in Nigeria: Prospects, challenges and opportunities. Journal of African Elections, 22(2). https://doi.org/10.20940/JAE/2023/v22i2a4
[75] Ibid
[76] IEBC Media Briefing <https://www.iebc.or.ke/uploads/resources/JqmDO7vRL0.pdf>
[77] Japheth Ondiek and Gedion Onyango, 'Realising digitalised electoral process in Africa: Public policy implications from Kenya's electoral technology systems' (Tayarisha Working Paper Series: September 2023) available at <https://wiredspace.wits.ac.za/server/api/core/bitstreams/ee26f3ec-0111-4259-abbc-16436877b0bf/content> accessed May 14, 2024.
[78] TikTok Launches Kenyan General Election Guide In-App as Part of Its Peace and Safety Initiative' (Newsroom | TikTok, 16 August 2019) <https://newsroom.tiktok.com/en-africa/tiktok-launches-kenyan-elections-hub> accessed 14 May 2024.

Crunching the Numbers: Analysis from Survey Findings from Electorates in Nigeria and Kenya

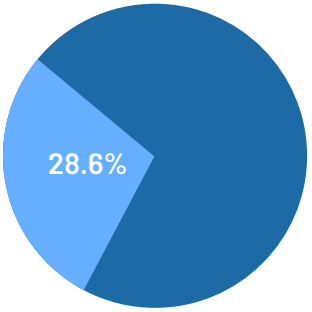
In line with the research goals of offering recommendations to address data governance concerns in the electoral processes of Nigeria and Kenya, this report conducted an online survey through Google Forms and held virtual focus group discussions to collect responses from electorates in these regions. The survey questions were designed in accordance with existing literature relating to electorate experiences, concerns, complaints, and factors impacting or influencing their participation in elections. The questions mostly required "yes," "no," or "unsure" responses, with a few exceptions that required direct responses from the focus groups. The responses from the survey form the basis of the discussion in this part.

Common features observed include a general lack of trust in electoral institutions' data governance practices. Analysis of responses shows a common expression of displeasure, although this is mostly tied to concerns about data security, privacy violations, and misuse of personal information. Other electorate concerns include excessive data collection, lack of transparency, unsolicited political communication, and various forms of discrimination based on political choice. Further findings from the survey and focus group discussions are documented below through charts and visualisations.

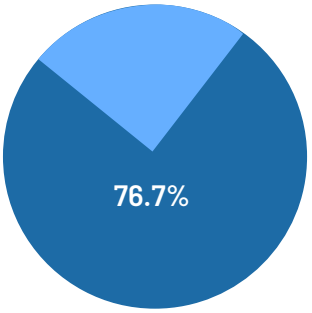
Details of Survey Findings from Electorates in Nigeria and Kenya

A total of 129 responses were collected to form the basis of this analysis.
The survey revealed that:

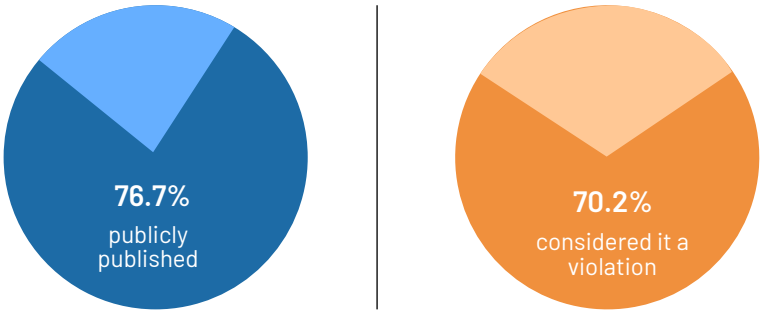
- **Confidence in data protection:** Only **28.6%** of the participants expressed confidence that the Electoral Commission can adequately protect their data. This low level of confidence underscores the urgent need for electoral bodies to strengthen their data protection measures to build trust among voters.



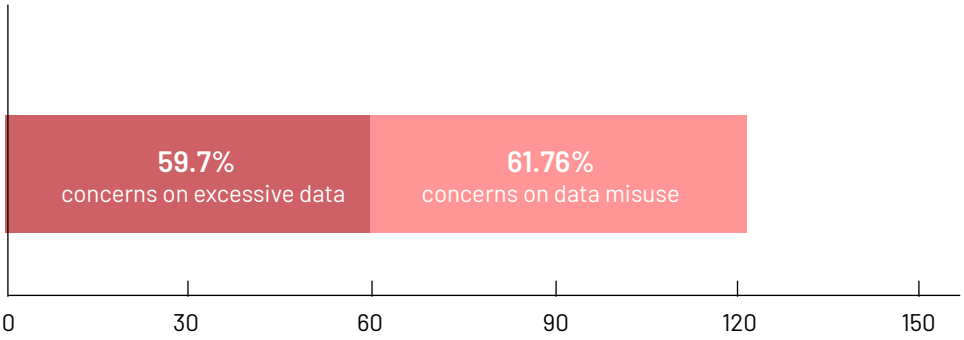
- **Impact of data security on voter participation:** A significant **76.7%** of participants agreed that more people would be willing to participate in elections if the issue of data security is addressed. This indicates that enhancing data protection could lead to higher voter turnout and greater electoral engagement.



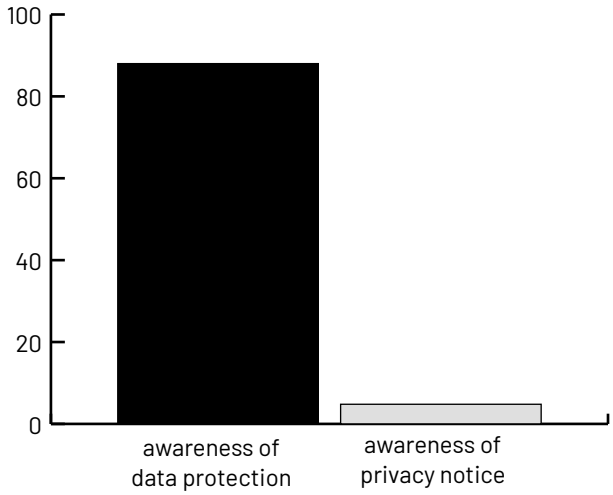
- **Privacy violations and public data publication:** Alarmingly, **78.3%** of the participants reported that their data were publicly published at polling units, and **70.2%** considered this a violation of their privacy. Such practices breach privacy rights and deter voter participation due to fears of exposing personal information.



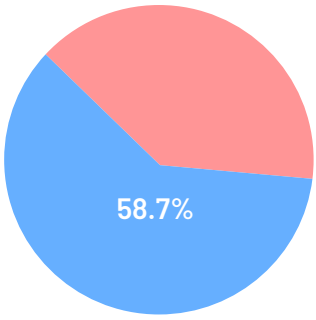
- **Excessive data collection and misuse: 59.7%** of the participants raised concerns about excessive data collection, while **61.76%** believed that their data were used for purposes other than what was initially intended. This misuse of data highlights the need for stricter regulations and transparency in data handling by electoral bodies.



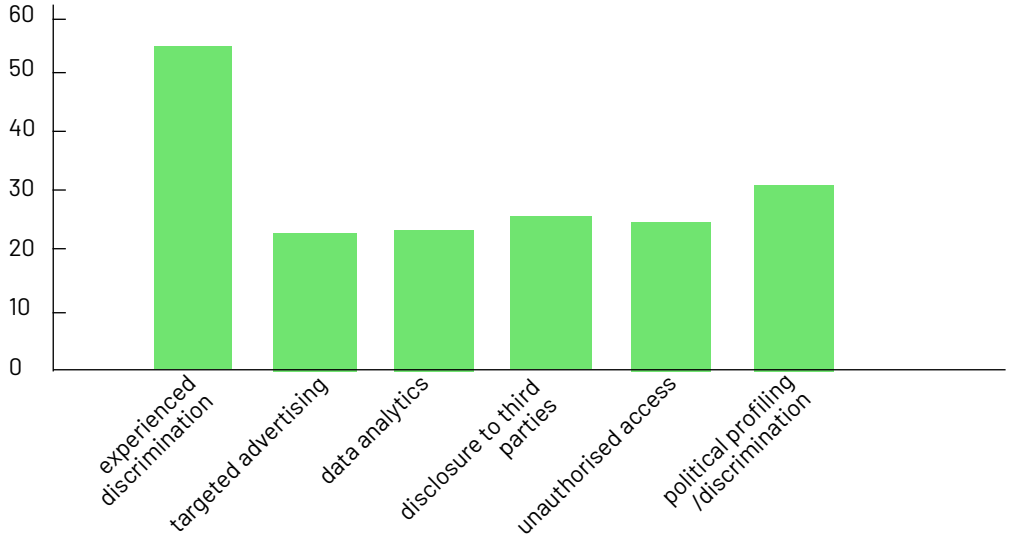
- **Transparency and awareness education on data protection:** A resounding **88%** of participants emphasised the need for increased voter awareness, particularly regarding data protection rights. Only **4.8%** were aware of the privacy notice of their electoral commission, indicating a significant gap in communication and education.



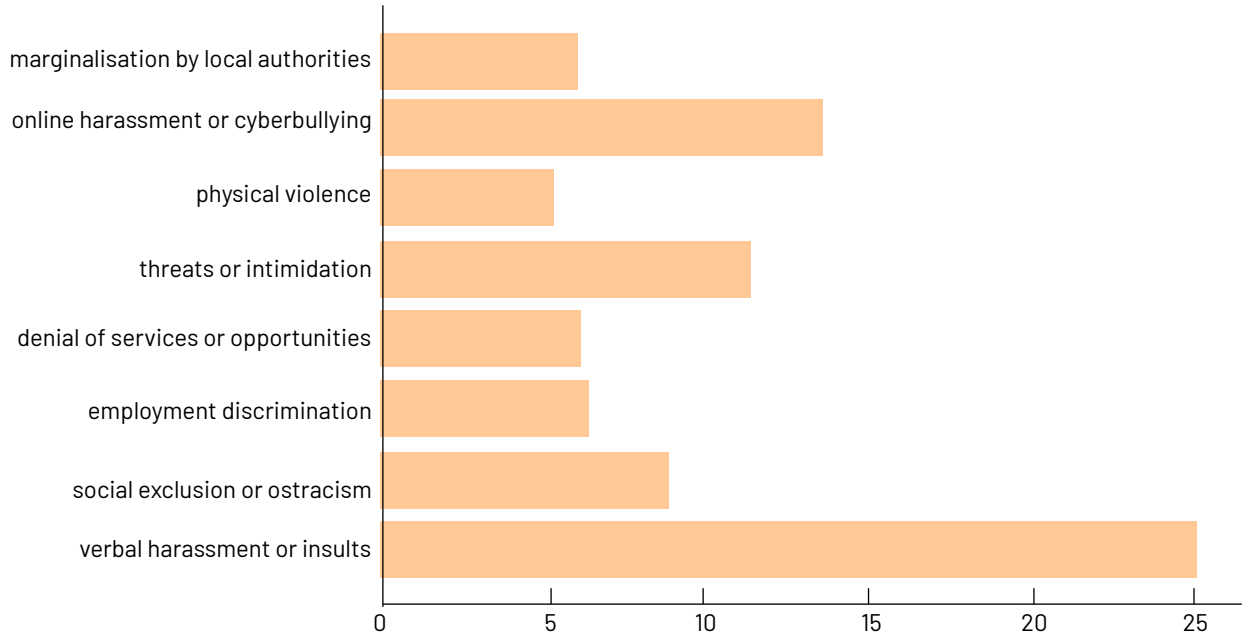
- **Unsolicited political communication:** Post-voter registration, **58.7%** of participants received phone calls from political parties soliciting votes, raising concerns about the unauthorised use of personal data for campaign purposes.



- **Discrimination and unlawful data Processing:** More than half **(54.2%)** of the participants reported experiencing discrimination pre- or post-election. Additionally, **unlawful processing of data was reported in various forms:** targeted advertising **(22.8%)**, data analytics for non-electoral purposes **(23.2%)**, disclosure to third parties **(24.93%)**, unauthorised access **(24.5%)**, and political profiling/discrimination **(30.7%)**.



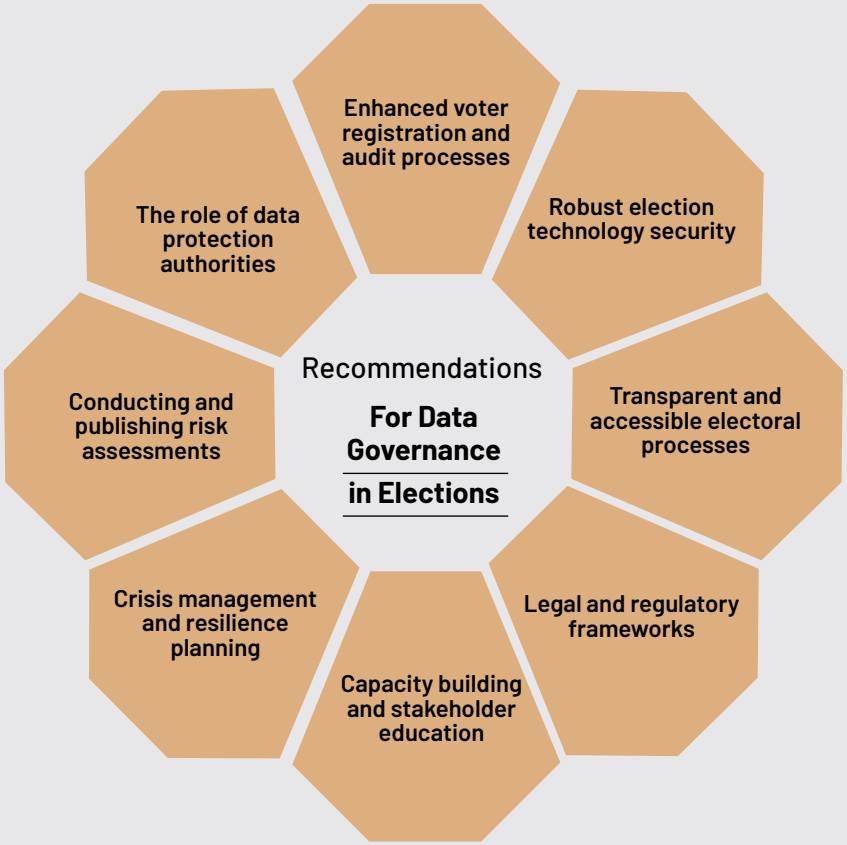
- **Forms of discrimination based on political choice:** Participants faced various forms of discrimination based on their political choice, including verbal harassment or insults **(25.03%)**, social exclusion or ostracism **(8.8%)**, employment discrimination **(6.37%)**, denial of services or opportunities **(6.1%)**, threats or intimidation **(11.4%)**, physical violence **(5.3%)**, online harassment or cyberbullying **(13.5%)**, and marginalisation by local authorities **(5.97%)**.



These findings reveal critical areas where electoral bodies in Nigeria and Kenya must focus their efforts to protect voter data and privacy, thereby fostering a more secure and inclusive electoral environment.

Recommendations and Best Practices for Data Governance in Elections

The case studies from Nigeria and Kenya highlight the critical importance of effective data governance in electoral processes. These elections exposed significant data management, security, and transparency challenges, impacting the legitimacy of election outcomes and public trust in democratic institutions. This section outlines best practices and key lessons learned from these experiences. By adopting these recommendations, countries can enhance electoral integrity, ensure the protection of voter information, and reinforce the overall credibility of their electoral systems. These practices are not only crucial for Nigeria and Kenya but also provide valuable insights for improving election data governance in Africa. These include the following:



Enhanced voter registration and audit processes

This can be achieved through efficient biometric registration processes and regular audits. Implementing biometric systems can significantly reduce issues of duplicate registrations and voter impersonation. Both Nigeria and Kenya have initiated biometric registration, which should be continually updated and audited to ensure accuracy and integrity. Similarly, conducting regular audits of the voter rolls to remove inaccuracies, such as deceased individuals or duplicate entries, is crucial. This practice ensures up-to-date data and boosts public confidence in the electoral process.

Robust election technology security

Enhancing the security of the technology deployed in processing voter data is critical to effective data governance. Ensuring that all data, especially electronically transmitted results, is encrypted can safeguard against tampering. Secure channels for data transmission must be established and tested extensively before election day. Additionally, to ensure transparency and integrity, implementing systems that allow for independent verification of election results, such as blockchain technology, could provide a transparent and tamper-proof method of result transmission and storage.

Transparent and accessible electoral processes

Transparency and availability are key elements of data governance, which must be guaranteed. Providing stakeholders, including political parties, civil society, and the public, access to electoral data such as voter lists and real-time results can enhance transparency. However, the provision of voter lists should be carried out with privacy considerations to ensure that personal data is not exposed to the public. Real-time public results sharing as they are collected not only increases transparency but also reduces the likelihood of result manipulation during the collation process.

Legal and regulatory frameworks

Developing comprehensive legal frameworks that cover all aspects of data governance in elections, including data protection, security, interoperability, data classification, access rights, and penalties for data manipulation, is essential.[79] The regulatory authorities also have a critical role to play through proper enforcement of existing laws and regulations to ensure all parties adhere to established data governance standards. Additionally, electoral agencies charged with conducting elections must ensure compliance with existing frameworks for data protection in the election processes.

Capacity building and stakeholder education

As people make up the entire data governance spectrum, it is important to equip them with the required skills and knowledge. Regular training for electoral officials on the latest data governance practices and technologies is crucial. This training should also extend to security protocols and emergency response strategies. On the other hand, educating the public about their rights and the measures in place to protect their data is vital for maintaining trust in the electoral process.

Crisis management and resilience planning

Resilience is an important aspect of security and data governance. Robust backup systems and contingency plans for election technology are essential. These plans should be well-documented and rehearsed to ensure quick recovery from any form of data loss or corruption. Regular stress tests and simulations of the electoral system can help identify vulnerabilities before an election, allowing for timely remediation.

[79] Damian Eke, et al, 'Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs', <https://www.researchgate.net/publication/363157320_Responsible_Data_Governance_in_Africa_Institutional_Gaps_and_Capacity_Needs> accessed 14 May 2024.

Conducting and publishing risk assessments

To ensure the integrity and security of electoral processes in the face of emerging technologies, it is recommended that a comprehensive risk assessment be conducted for all new technologies utilised in elections before deployment. This assessment should identify potential risks to data protection and electoral integrity, evaluate the likelihood and impact of these risks, and propose mitigation strategies to address them. Conducting and publicly publishing assessments such as Privacy Impact Assessment (PIA), Human Rights Impact Assessment (HRIA) and Data Protection Impact Assessment (DPIA) promotes transparency and accountability, fostering public trust in the electoral process. Nigeria conducted such an assessment in 2009, but it has not done the same recently.[80] Additionally, continuous monitoring and periodic reviews should be implemented to adapt to evolving threats and technological advancements, ensuring the ongoing protection of electoral data.

The role of data protection authorities

DPAs play a critical role in ensuring the protection of personal data during elections. Some DPAs in countries like Kenya, Senegal, and South Africa have developed guidelines for compliance with data protection laws during elections. These provide a framework for electoral bodies and political parties to ensure the privacy and security of voters' data in the electoral process. Thus, other DPAs in countries like Nigeria must follow suit, publish comprehensive data protection guidelines during elections, and create awareness of effective data management before every election.

Conclusion

The analysis of data governance practices within the electioneering processes of African countries, with a particular focus on Nigeria and Kenya, sheds light on the pivotal role effective data management plays in ensuring the credibility, transparency, and integrity of democratic elections. Through an exploration of global best practices and insights gleaned from the experiences of these nations, it becomes evident that robust data governance frameworks are essential for preserving the sanctity of electoral processes.

The examination of the electioneering processes in Kenya and Nigeria has underscored the far-reaching implications of inadequate data governance practices. From irregularities in data transmission to compromised electronic voting systems, these elections serve as sobering reminders of the urgent need for transparent, verifiable, and secure management of electoral data. Moreover, they highlight the profound impact of data governance failures on electoral outcomes, public trust, and the credibility of democratic processes.

[80] National Identity Management Commission, 'Privacy Impact Assessment Report Executive Summary' (2009) https://nimc.gov.ng/pia_report.pdf accessed 9 June 2024.

Amidst these challenges, there is a clear imperative for action. Strengthening legal and regulatory frameworks, investing in robust election technology security measures, and prioritising capacity building and stakeholder education are critical steps towards enhancing data governance in electoral processes. By adopting these recommendations and learning from global best practices, African countries can fortify their electoral systems, uphold democratic principles, and foster trust among citizens.

Ultimately, the research underscores the intertwined nature of data governance and democracy in the digital age. As technology continues to reshape electoral landscapes, ensuring the responsible, transparent, and accountable management of data is paramount. By embracing this ethos and embracing data governance as a cornerstone of electoral integrity, Nigeria, Kenya, and other African nations can forge a path towards resilient, inclusive, and credible democratic governance.

IKIGAI

DATAFICATION AND DEMOCRACY FUND

TECH HIVE ADVISORY