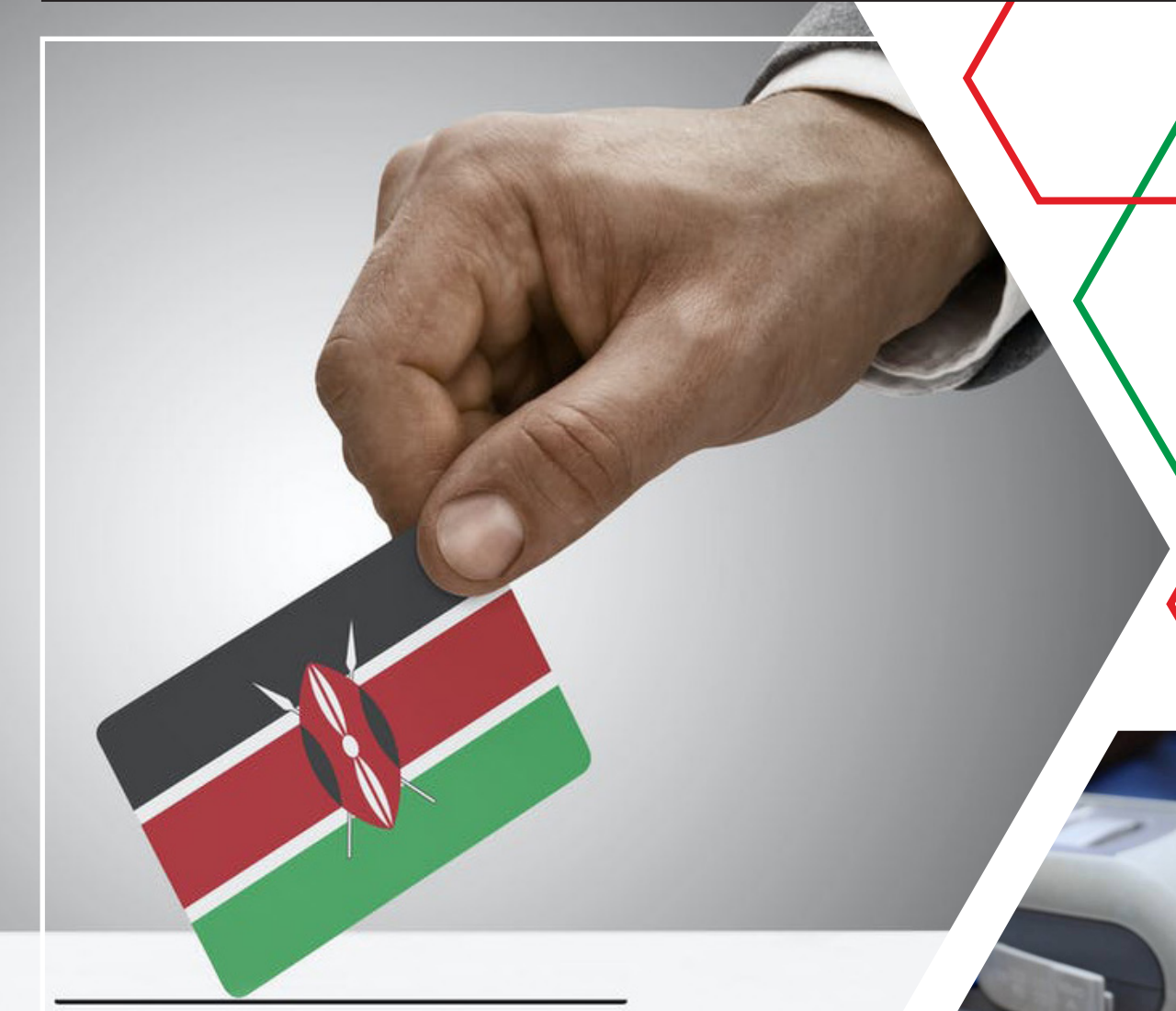

Personal Data & Elections 2022

By Tevin Mwenda and Victor Kapiyo

KICTANet
The Power of Communities
www.kictanet.or.ke

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.orke
Web: www.kictanet.or.ke
TWitter: @kictanet

Project title:
The Advocating for Data Accountability, Protection and Transparency (ADAPT) Project

Sponsor:
Internews

Authors:
Tevin Mwenda and Victor Kapiyo

Design & Layout:
Stanley Murage (stanmuus@gmail.com, Cell:+254 720316292)

Location and year of publication: Nairobi 2022
Policy Brief No.9, February 2022

Table of Contents

Executive Summary

The aim of this brief is to assess how the implementation of the Data Protection Act, 2019 will impact the 2022 Kenyan elections. The importance of this law is that unlike previous elections, the 2022 election will be the first to be held with a comprehensive data protection law in place.

The brief reviews the collection and processing of personal data during the stages of the election cycle as identified by the Independent Electoral and Boundaries Commission which include: legal framework, planning and implementation, training and education, voter registration and nominations, electoral campaign, voting operations and election day, verification of results and post-elections.

It then proceeds to identify the data protection challenges that have arisen at these stages, and highlights key risks to the collection and processing of data. The paper also demonstrates how the Data Protection Act will affect the processes and the various stakeholders in the 2022 election.

Accordingly, this brief finds that even though the Data Protection Act and its constituent regulations are in place, the key stakeholders that are part of the election cycle are yet to update their procedures to align them to the Act. This is of particular concern given the potential challenges and risks posed to personal data during an electoral process. The absence of adequate data protection measures, in the absence of remedial measures to remedy the situation, could result in privacy violations in the processes leading up to the August election.

In this regard, the brief makes the following key recommendations:

a) **Election management bodies including the IEBC, ORPP and political parties should urgently have in place comprehensive data protection policies and comply with the Data Protection Act, 2019 at all stages of the election cycle, including conducting data protection impact assessments.**

b) **The ODPC should provide effective and independent oversight on the data collection and processing operations of the various election management entities, including developing guidelines for the handling of personal data during electoral processes.**

c) **Telecommunication companies and other third party technology companies facilitating the election should adopt privacy and security by design and default in all their systems to be used for collection and processing of personal data of voters.**

d) **The public should be educated to enable them to cultivate a value system that promotes respect for the right to privacy.**

e) **Civil society should continue to monitor the implementation of the Data Protection Act by all stakeholders during the electoral process.**

1 Introduction & Background

In the past decade, elections in Kenya have become more about voting. Today, the entire election cycle which includes the legal framework, planning and implementation, training and education, voter registration and nominations, electoral campaign, voting operations and election day, verification of results and post-elections are increasingly data dependent with the use of digital technology to aid the collection, storing and analysis of personal data.[1]

The collection and processing of personal data is undertaken by various election stakeholders including among others, the Independent Electoral and Boundaries Commission (IEBC), the Office of the Registrar of Political Parties (ORPP), state security agencies, the Judiciary, political parties, politicians, media, telecommunication providers and civil society.

Instructively, the IEBC in the elections collected and processed the personal data of 19,611,423 voters, of which 47% were female and 53% were male, while 51% were aged between 18-35 years.[2] Further, the Commission also collected and processed personal data of 14,523 candidates who contested in the August 2017 election.[3] The voter turnout for the election was 78% as compared to 86% recorded in 2013.[4] The IEBC expects to spend an estimated KES 40.9 billion (USD 361.3 million) for the 2022 election[5] and register an additional 7 million new voters.[6]

The reliance of elections on the mass collection of personal data and its processing through digital technologies presents new challenges that were previously not anticipated. Biometric data collection by the election management body, the national government's Huduma Namba and political parties increases the risks to the privacy of personal data, especially considering the role of third-party contractors hired to develop and deploy data collection technologies.

Likewise, the collection of personal data by political parties and its use to drive campaigns, for political strategy, targeting and campaign messaging including on social media could present opportunities for abuse. Moreover, the increased use of digital technologies and connected devices over the internet to relay

1. Voter Education Training Manual, https://www.iebc.or.ke/uploads/resources/pdQMe3WKeV.pdf
2. IEBC, 'IEBC Data Report of 2017 elections', https://www.iebc.or.ke/uploads/resources/siEABKREDq.pdf
3. Ibid
4. Ibid
5. Citizen TV, 'IEBC chairman Chebukati says the commission needs Ksh 40.9 B for elections' (Citizen TV, August 2021), https://www.youtube.com/watch?v=j0ldLOBZ60A
6. KTN News, 'Elections Countdown: All eyes on IEBC as it prepares for the 2022 General elections' (KTN News, August 2021), https://www.youtube.com/watch?v=5EpNBR0PbKU&t=211s

this information also presents new cybersecurity risks if systemic and human vulnerabilities are not addressed. Collectively, gaps in the handling of personal data could undermine the electoral process, leading to a loss of confidence in democratic institutions.

Notably, the adoption of the Data Protection Act, 2019 which aims to buttress the right to privacy under article 31 of the Constitution of Kenya, 2010, and the establishment of the Office of the Data Protection Commissioner (ODPC) presents a stellar opportunity to safeguard the right to privacy in Kenya from an elections context. The aim of this brief is to consider the implications of this legislation on the election cycle and present some insights on how stakeholders could address the privacy risks that arose in previous elections.

1.1 Methodology

The study uses a mixed approach. The research commenced with a desktop review of relevant literature, including policies, laws, regulations, decided cases, reports, news articles and other documents from Kenya, and other relevant jurisdictions.

Also, relevant information was gathered from feedback obtained during events such as the Kenya Internet Government Forum (KIGF) held on 23 September 2021 and the Konrad Adenauer Stiftung workshop on 'Internet As A Democratic Tool in Kenya' held between 28 September to 30 September 2021.

2 Legal Framework on Election & Personal Data in Kenya

2.1 Constitution of Kenya, 2010

The basis for elections and the collection of personal data is provided for under the constitution. Firstly, it grants all sovereign power to the people,and empowers them to exercise it either directly or through their democratically elected representatives.[7] Secondly, it provides for the right of every citizen to free, fair and regular elections based on universal suffrage and the free expression of the will of the electors, and of every adult citizen to be registered as a voter and to vote by secret ballot in any election or referendum.[8]

Further, article 31 provides for the right to privacy, including the right not to have information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.[9]

In addition, the constitution requires Parliament to enact legislation to provide for the continuous registration of citizens as voters; the conduct of elections and referenda and the regulation and efficient supervision of elections and referenda, including the nomination of candidates for elections.[10] Further, to come up with legislation on political parties including the regulation of freedom to broadcast to ensure fair election campaigning; the regulation of political parties, the roles and functions of political parties, the registration and supervision of political parties and any other matters necessary for the management of political parties.[11]

Also, it mandates the conduct of general elections every five years, or whenever vacancies within the elective offices at the national and county level.[12] Lastly, it mandates the IEBC to conduct and supervise referenda and elections to any elective body or offices established by the Constitution, and any other statute.[13]

2.2 Elections Act, No. 24 of 2011

The Election Act mandates the IEBC to compile and maintain voter registers including, poll, ward, constituency, county registers and a register of voters residing outside Kenya.[14] Further, the Commission is required to carry out continuous voter registration and review,[15] including by regularly revising and updating the register of voters. These processes involve the collection and processing of data for purposes of conducting elections.

7. Constitution of Kenya 2010, art. 1
8. Constitution of Kenya 2010, art. 38
9. Constitution of Kenya 2010, art. 31
10. Chapter 7
11. Constitution of Kenya 2010, art. 92
12. Constitution of Kenya 2010, art. 101, 136, 172, 180,
13. Constitution of Kenya 2010, art. 88
14. Election Act 2011, s. 4, https://www.iebc.or.ke/uploads/resources/kqI5cmgeyB.pdf
15. Election Act 2011, s. 5

Furthermore, the IEBC is required to make the register of voters accessible to the public for inspection at all times for the purpose of rectifying it, and for verification prior to an election.[16] The Act does not state the nature of the data the IEBC should reveal to the members of the public, or the extent of access voters may have of the personal data in the register.

Section 44 of the Act requires the IEBC to use such technology as it considers appropriate in the electoral process, including in the collection and processing of election data. The Act was amended[17] in 2016, to establish the integrated electronic electoral system which collects and processes personal data under its key components such as biometric voter registration, biometric voter identification and electronic result transmission system. [18]

2.3 Independent Electoral and Boundaries Commission Act, 2011

The Act empowers the IEBC to collect and handle data on the elections, such as the continuous registration of voters, the revision of the voters' roll, the registration of candidates for elections,[19] voter education, the facilitation of the observation, monitoring and evaluation of elections, the development and enforcement of codes of conduct for candidates and parties contesting elections, and the use of appropriate technology to performance its functions.[20]

Section 25 of the Act was amended in 2019 and now requires that the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters.[21]

2.4 The IEBC Elections (Technology) Regulations, 2017

These regulations govern the use of technology in elections and their use to collect, process and store election data.[22] The regulations defines election technology as "a system that includes a biometric voter registration system, a biometric voter identification system, a system that enables the nomination and registration of candidates and an electronic results transmission system.[23]

They also define the term "biometric" to mean the "unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures", and "data" as "an attribute to an entity recorded in a format in which it can be processed to produce information by equipment in response to instructions given for that purpose, and includes representations of facts in form of quantities, characters, symbols and images, transmitted in the form of electrical signals and stored on magnetic, optical or mechanical recording media or as defined in the Kenya Information and Communication Act, 1998." Moreover, the regulations highlight how election technology should be acquired, stored and deployed[24] and mandates the IEBC to conduct tests on the technology to ensure they work as required. [25]

Also, the IEBC is required to ensure its data is backed up, stored securely, kept separate from the main data, retain election data for three years after the elections, and to have a timely data recovery plan in case of data breaches.[26]

16. Ibid, s 6
17. The Election Laws (Amendment) Act, 2016, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2016/No._36_of_2016.pdf
18. The Election Laws (Amendment) Act, 2016 s 17
19. Independent Electoral and Boundaries Commission Act 2011, S. 4, https://www.iebc.or.ke/uploads/resources/8Z5fmROhVD.pdf
20. Ibid
21. Ibid, s. 25
22. IEBC Elections (Technology) Regulations, 2017, Part 1, https://www.iebc.or.ke/uploads/resources/8IJsH5aTCd.pdf
23. bid
24. Ibid, Part 2
25. Ibid, Part 3
26. Part VI and IX

The regulations also require the IEBC to work with telecommunication network providers to ensure that there is sufficient network coverage to facilitate the use of election technology for voter validation and results transmission.[27] The regulations have yet to be amended to provide comprehensive guidance for the protection of personal data collected and processed through election technology in line with the Data Protection Act, 2019.

2.5 Political Parties Act, 2011

The Act empowers the Office of the Registrar of Political Parties (ORPP) and political parties to collect and process data of their members. Section 17 of the Act requires political parties to maintain an accurate and authentic register of its members in the form prescribed in the Second Schedule.[28]

The membership details required to be contained in the register include identification details, region, ethnicity, gender and county. At the time of registration, applicants are required to submit a list of at least 1,000 members in a majority of the counties (at least 24,000 members) who should reflect regional and ethnic diversity, gender balance and representation of minorities and marginalised groups.

Section 39 of the Act mandates the Office of the Registrar of Political Parties to verify and make publicly available the list of all members of political parties; maintain a register of political parties and the symbols of the political parties; and ensure and verify that no person is a member of more than one political party and notify the Commission of his findings.

27. Ibid VIII

28. Political Parties Act 2011, s. 17, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/PoliticalPartiesAct.pdf

3 Data Protection Challenges in the Election Cycle

This section reviews the data protection challenges in the various stages of the elections cycle as categorised by the IEBC such as: planning and implementation, training and education, registration and nomination, electoral campaign, voting operations and election day, verification of results and post-elections.

3.1 Planning & Implementation

This stage involves budgeting, procurement of election material, recruitment of election officials. It is at this stage that all they key election personnel posts such as: the Commissioners, the Secretariat constituting the Commission Secretary and Chief Executive Officer (CS/CEO), Deputy Commission Secretary (DCS), 9 Directors, 24 Managers, 47 County Election Managers and 290 Constituency Election Coordinators are filled. [29]

During the procurement for materials, the challenge that has arisen is the procurement of technology that does not work as expected. For example, in 2017 the Electronic Voter Identification systems failed to work as expected on election day,[30] and in some instances, they were not able to identify voters.[31]

The IEBC is currently in the process of procuring technology suppliers including to maintain the Kenya Integrated Elections Management System (KIEMS) software.[32] According to the Commission, the upgrades are necessary as the server hosting the Biometric Voter Registration system acquired in 2012 cannot accommodate that data of more voters, while the system needs to include iris identification.[33] However, the IEBC has not publicly provided any information regarding the privacy standard that they will require the software provider to adhere to, or the privacy by design measures that the successful vendor should take into account in providing the system.

3.2 Training and Education

As part of its mandate, the IEBC conducts training to its officials and voters on the electoral process, to which end, it has published a Voter Education Training Manual.[34]

A key challenge with the manual is that it does not contain any: content on privacy and data protection; or official guidance on the steps that should be taken to mitigate data breaches during the election cycle. In the absence of this there have been incidents of concern. For example, in the run-up to the 2017 elections, it emerged that some IEBC officials were selling a voter's personal data including phone numbers, ID numbers, photos, age and polling stations to politicians for three shillings. [35]

29. IEBC Secretariat https://www.iebc.or.ke/iebc/?secretariet
30. Ibid
31. Ibid
32. Moses Odhiambo 'IEBC dilemma in multi-billion poll kits tender' (The Star, May 2021), https://www.the-star.co.ke/news/2021-05-12-iebc-dilemma-in-multi-billion-poll-kits-tender/
34. Ibid
35. Voter Education Training Manual, https://www.iebc.or.ke/uploads/resources/pdQMe3WKeV.pdf

3.3 Registration and Nominations

The current Biometric Voter Registration System comprises both voter registration and voter identification. During registration, the system[36] captures a voter's fingerprints, their photo and their Identification Card alongside other personal information such as the location they will be voting at. For voter identification, the Electronic Voter Identification System (EVID) which is an electronic poll book is used.[37] There EVID comprises either a laptop with an attached fingerprint reader,[38] or the handheld device with an in-built fingerprint reader. The EVID is used to verify and confirm a voter's identity electronically as registered by the Biometric Voter Registration System (BVR).[39]

Previously, the challenges reported included the misuse of the data collected using the biometric voter registration system, the lack of a clear hierarchy of access to data, the level of access and cyber security concerns. Section 6 of the Elections Act requires the IEBC to have the voter register opened for inspection by members of the public at all times for the purpose of rectifying the particulars.

However, the modalities for ensuring the privacy of the information in the register remains problematic given the amount of personal information contained in the register. In January 2017, the IEBC suspended the SMS query 22464 to the voter registration database citing problems with the system and voter anxiety.[40] It also disabled the voter verification official website portal,[41] after privacy concerns were raised by stakeholders including KICTANet. However, by disabling both services, the Commission has effectively denied voters access to a mechanism to quickly access, verify and update their personal information.

Moreover, a report by the Centre of Intellectual Property and Information Technology (CIPIT),[42] identified various instances where voters complained of receiving unsolicited messages from political parties and politicians urging them to go vote for them.[43] However, these voters had not consented nor shared their data with political parties for purposes of receiving political messages. The report also noted that the IEBC granted access to its election database at a fee, however, they redacted information such as phone numbers, ID numbers and polling stations.[44]

The practice raises the question of how to balance between the right to access information and safeguard the privacy of voters' personal information. With respect to cybersecurity, the IEBC is required under the IEBC Elections (Technology) Regulations, 2017, to put in place mechanisms to ensure data availability, accuracy, integrity, and confidentiality.[45] However, in July 2021 there were reports of hacking of the IEBC database in which it is estimated that the personal data of 61,617 registered voters from a county in western Kenya were compromised.[46]

Currently, the IEBC has been undertaking a mass voter registration drive in January 2022 which will be relying on the biometric kits used in the 2017 elections and recent by-elections.[47] The IEBC is expected to audit the voter register which

---

36. Brian Wasuna 'How rogue IEBC staff minted cash from sale of voters' data' (The Star, 10th May 2018), https://www.the-star.co.ke/news/2018-05-10-how-rogue-iebc-staff-minted-cash-from-sale-of-voters-data/

37. IEBC, 'Biometric Voter Registration System', https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR)

38. Raila Amolo Odinga & Another v Independent Electoral and Boundaries Commission & 2 others [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/140716/

39. Ibid

40. Ibid

41. IEBC suspends SMS query by voters, https://hivisasa.com/posts/iebc-suspends-sms-query-by-voters; IEBC Twitter, https://twitter.com/iebckenya/status/822114741564874753; IEBC Press Release, https://www.iebc.or.ke/uploads/resources/bHOtKVoeKT.pdf IEBC Voter Verification Portal, http://voterstatus.iebc.or.ke/voter

42. Dr Robert Muthuri Francis Monyango, Wanjiku Karanja, 'Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 Election Process' (Center of Intellectual Property and Information Technology, May 2018), https://cipit.strathmore.edu/biometric-technology-elections-and-privacy-investigating-privacy-implications-of-biometric-voter-registration-in-kenyas-2017-election-process/

43. Ibid

44. Ibid

45. Ibid, s. 14

46. Cyrus Ombati, 'Suspect hacked IEBC database, stole 61,000 names for fraud — DCI' (The Star, July 2021), https://www.the-star.co.ke/news/2021-07-17-suspect-hacked-iebc-database-stole-61000-names-for-fraud-dci/

47. KTN News, 'Exploring the preparedness and the key timeliness of the IEBC to conduct the 2022 General Elections' (KTN News, August 2021), https://www.youtube.com/watch?app=desktop&v=d6ouQOYi_7I

involves verifying and ensuring that the data they have is accurate.[48]

3.4 Electoral Campaign

In the run up to an election, political parties conduct campaigns and rallies to urge people to vote for candidates from their respective parties. Increasingly, political parties are now using social media for publicity and campaigns which present new challenges.

These include the use of such platforms to conduct data scraping where social media user data is acquired to profile potential voters for purposes of sending them targeted advertisements that are aligned with what the voters want to hear, to spread misinformation and propaganda. Political parties also send unsolicited SMS messages to voters without their consent.

The Cambridge Analytica scandal exemplified the extent to which political parties such as the Jubilee Party in Kenya used social media platforms such as Facebook to manipulate voters through targeted messages and advertisements to popularise their candidates and disseminate political messages.[49] The company used social media for propaganda, misinformation and disinformation by among others actively painting the other candidates in a bad light. According to the then CEO of Cambridge Analytica, Alexander Nix, things "don't necessarily need to be true as long as they are believed."[50]

In addition, a 2021 report by the Mozilla Foundation showed how Kenyan journalists, judges, and other members of civil society had faced coordinated disinformation and harassment campaigns on Twitter and that Twitter had done little to stop the practice.[51] The research uncovered nine different disinformation campaigns involving 23,000 tweets with 3,700 participating accounts. Further, social media influencers were paid between USD 10 to 15 daily to participate in disinformation campaigns on Twitter to ensure the messages trended.[52] As we approach an election in 2022, it is likely that such approaches and tactics may be replicated on social media platforms.

Also, some political parties obtained data from the IEBC and other sources such as M-Pesa agents which information was used to send unsolicited SMS messages to the public. In the run-up to the 2017 elections, political parties relied on data for their targeted political campaigns, disinformation, and political messages.[53] Thus, personal data was obtained from the IEBC register and was used to send bulk SMS messages via telecommunication platforms.

These SMS messages urged voters to go vote for their respective candidates. Data subjects complained that they were receiving unsolicited messages from political parties and politicians.[54] It is noteworthy that the data subjects had neither consented nor shared their data with political parties for purposes of receiving political messages.[55] This begged the question of how the political parties accessed the sensitive election data.

Consequently, in June 2021, there was uproar when many members of the public discovered that they had been registered to various political parties without their consent.[56] This was only discovered after the Office of Registrar of Political Parties created a portal enabling the public to check which parties they belonged to.[57]

48. Ibid
49. Larry Madowo, 'How Cambridge Analytica poisoned Kenya's democracy' (Washington Post, March 2018), https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/
50. Ibid
51. Odanga Madung and Brian Obilo, 'Inside the shadowy world of disinformation for hire in Kenya' (2021) Mozilla Foundation, https://foundation.mozilla.org/documents/221/Report_Inside_the_shadowy_world_of_disinformation_for_hire_in_Kenya_5._hcc.pdf
52. Ibid
53. Dr Robert Muthuri Francis Monyango, Wanjiku Karanja, 'Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 Election Process' (Center of Intellectual Property and Information Technology, May 2018), https://cipit.strathmore.edu/biometric-technology-elections-and-privacy-investigating-privacy-implications-of-biometric-voter-registration-in-kenyas-2017-election-process/
54. Ibid
55. Ibid
56. Julius Otieno, 'Kenyans protest registration as party members without consent (The Star, June 2021), https://www.the-star.co.ke/news/2021-06-19-kenyans-protest-registration-as-party-members-without-consent/
57. Ibid

The Registrar of Political parties clarified that it was not their obligation to register members to a political party, as the role belonged to political parties.[58] Subsequently, the Registrar closed the portal for a period following the intervention of the ODPC, thus denying those who have not yet accessed the portal to confirm the registration status.[59] However, the portal has since been restored on the eCitizen portal and people can now verify their registration status, and resign from parties where they find themselves wrongly registered.[60]

3.5 Voting Operations and Election Day

At this stage, the key processes include voter identification and verification, voting and vote counting by the IEBC. The notable challenges that arose in 2017 included the failure of the Electronic Voter Identification systems and lack of transparency of how the technology worked, or how it was intended to work. In some instances, the electronic systems were not able to identify voters, resulting in the IEBC turning to the use of the printed copies of the voters register.

The failures around the electronic and printed registers were adjudicated upon during the 2017 presidential election petitions.[61]

The second challenge was the lack of transparency in how the technology worked and what it could deliver to ensure a fair election. This was seen when the Supreme Court ordered the IEBC to share the logs of the Electronic Voter Identification systems.[62] The purpose of this was for the court to be able to ascertain and verify the claims by the litigants regarding voter identification and electronic results transmission.

3.6 Verification of results

The IEBC is required to tabulate the results to verify that they are an accurate and true representation of the results. The electronic result transmission system was deployed in the 2017 elections[63] but, there were challenges when relaying election data results. Notably, the transmission system widely malfunctioned and an alleged programming error vastly inflated the number of legitimately rejected votes.[64] The IEBC entirely abandoned electronic tallying and opted only to use physical documents to tally the results.[65]

Moreover, there were reports that IEBC servers that were being used to store election data had been hacked although this was never proven.[66] The servers were not domiciled in Kenya. Further, the failures attributed to the transmission of presidential election results was one of the reasons cited by the Supreme Court in nullifying the results of the 2017 presidential election.[67]

58. Ibid
59. Political parties e-Citizen platform temporarily closed after online uproar, https://theinformer.co.ke/34006/political-parties-e-citizen-platform-temporarily-closed-after-online-uproar/
60. Office of the Registrar of Political Parties, https://orpp.ecitizen.go.ke/
61. Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 2 others [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/140716/
62. Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 2 others [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/140420/
63. The Election Laws (Amendment) Act, 2016, s. 2 and 5
64. Jonathan W. Rosen, 'How to Undermine a Democracy' (The Atlantic, December 2017), https://www.theatlantic.com/international/archive/2017/12/how-to-undermine-a-democracy/549089/
65. Ibid
66. Dr Robert Muthuri Francis Monyango, Wanjiku Karanja, 'Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 Election Process' (Centre of Intellectual Property and Information Technology, May 2018), https://cipit.strathmore.edu/biometric-technology-elections-and-privacy-investigating-privacy-implications-of-biometric-voter-registration-in-kenyas-2017-election-process/
67. Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 2 others [2017] eKLR,

3.7 Post-elections

The IEBC is required to audit and evaluate how the previous elections were conducted, update the voters list, propose legal reforms and undertake professional development of their teams. After the 2017 elections, the IEBC published a number of reports such as the KIEMS Report Logs by PollingStations[68] and a Data Report highlighting the election results of the various electoral posts.[69] However, the IEBC is yet to publish the KIEMS Report Logs for August 2017 presidential results.

In August 2021, the IEBC Chairperson Wafula Chebukati stated that the Commision was prepared to deploy and use technology in the transmission of results in the 2022 elections.[70] Some of the measures it had taken include: hosting the servers used for storing election data locally, and engaging local service providers to assist in the relaying results.[71] However, the Commission anticipated challenges in relaying results especially in areas that lack 3G coverage. To this end, they were engaging with the Communication Authority to find solutions to address the telecommunication network access gaps.[72]

68. KIEMS report, https://www.iebc.or.ke/uploads/resources/DjVeeev5d7.pdf
69. Data Report of 2017 Elections, https://www.iebc.or.ke/uploads/resources/siEABKREDq.pdf
70. KTN News, 'IEBC Chair Wafula Chebukati on the state of preparedness by the electoral body ahead of 2022 polls' (KTN News, August 2021), https://www.youtube.com/watch?v=EcMKLwVlpJk
71. Ibid
72. Ibid

4 Implications of the Data Protection Act on the Kenyan Election Cycle

This section reviews the key principles of data protection and their implications at various stages of the electoral cycle.

Article 31 of the Constitution of Kenya, 2021 provides that every person has the right to privacy.[73] Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which Kenya is a party to, states that no one shall be subjected to arbitrary or unlawful interference with his privacy. [74]

Following the enactment of the Data Protection Act 2019 and the establishment of the Office of the Data Protection Commissioner (ODPC), the 2022 elections will be conducted in an environment with a proper data protection policy, legal and institutional framework.

The ODPC has also published the Guidance Note on Processing Personal Data for Electoral Purposes (Guidance Note).[75] In addition, the Data Protection General Regulations 2021,[76] Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021[77] and Data Protection (Registration of Data Controllers And Data Processors) Regulations, 2021[78] will also affect how election data is handled in the upcoming general elections.

4.1 Principles of Data Protection

The Data Protection Act amended Section 25 of the Independent Electoral and Boundaries Commission Act to state that the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters. [79]

All the entities that will participate in the election cycle such as the IEBC, political parties, the ORPP, telecommunication providers, suppliers of election technology, election observers are bound by the principles of data protection under the Data Protection Act.

The principles of data protection are contained in section 25 of the Act.[80] These principles provide that personal data: should processed in accordance with the right to privacy of the data subject; processed lawfully, fairly and in a transparent manner; collected for explicit, specified and legitimate purposes; adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; collected only where a valid

73. Constitution of Kenya 2010, art. 31
74. International Covenant on Civil and Political Rights, art. 17
75. Guidance Note on Processing Personal Data for Electoral Purposes
76. The Data Protection General Regulations 2021,
77. The Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021,
78. The Data Protection (Registration of Data Controllers And Data Processors) Regulations, 2021
79. Data Protection Act 2019, Second schedule
80. Data Protection Act 2019, s. 25

explanation is provided whenever information relating to private affairs is required; accurate and, where necessary, kept up to date; kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The Guidance Note recognises that the data protection principles should be adhered to by the various parties handling election data. Even though all the principles apply to the various data collectors and processors in the election cycle, it is important to highlight critical principles in the handling of election data.

Right To Privacy

Data collectors and processors handling election data should ensure that they adhere to privacy as required under the constitution and the relevant data protection laws. Also, the election stakeholders involved in the registration and nomination, electoral campaign, voting operations and election day and verification of results should ensure that they adhere to the principle of privacy by design and default as required under the Data Protection Act and ensure that appropriate technical and organisational measures are taken in the systems they adopt. [81]

These measures should be designed to implement the data protection principles effectively and to integrate necessary safeguards for that purpose into the processing of personal data.[82] The Guidance Note acknowledges that election Stakeholders handle and share a vast amount of data and requires election stakeholders to take appropriate security measures to prevent accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. [83]

Further, the IEBC will need to ensure that when relaying election data over a telecommunication network, the service providers implement adequate security measures. Under the Data Protection Act, these measures should take into consideration: the state of technological development available; the cost of implementing any of the security measures; the special risks that exist in the processing of election data; and the sensitive nature of the data being processed. [84]

In addition, all stakeholders handling election data should ensure that the data is encrypted, pseudonymized and anonymized where possible; and that their systems are up to date and adequately secured. For example, they can consider conducting a red team exercise that is an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access, and also testing employees through several scripted social engineering and phishing tests. [85]

Moreover, the stakeholders should ensure that the third parties used to transmit or store data have the same technical and organisational measures to ensure that the data in their custody is secure.[86] Further, election stakeholders should ensure that such third parties have the ability to protect personal data and maintain its confidentiality.[87] They should be obliged to conduct a risk assessment on the ability of the third party to protect the data, which assessment should seek to achieve outcomes that embed high standards of security throughout the processing.[88] The Data Protection (General) Regulations require that election data should be stored in Kenya.[89]

81. Ibid
82. Ibid
83. Guidance Note on Processing Personal Data for Electoral Purposes, s. 11
84. Ibid, s. 42
85. What are red team exercises under the CBK guidance notes on cybersecurity? CIPIT, https://cipit.strathmore.edu/what-are-red-team-exercises-under-the-cbk-guidance-notes-on-cybersecurity/ accessed 13th September 2021
86. Ibid, s.42
87. Guidance Note on Processing Personal Data for Electoral Purposes, s. 11
88. Ibid
89. Data Protection (General) Regulations 2021, s. 25, http://161.35.8.237:8080/wp-content/uploads/2021/06/Data-Protection-General-regulations.pdf

Accurate and kept up to date

Both the Data Protection Act and the Election Act require that personal data is up to date and accurate.

Under the Data Protection Act, data subjects have the right to the correction of false or misleading data; and to deletion of false or misleading data about them. This also applies to election data.

The IEBC and political parties ensure this by continuously updating the voters' and members' registers respectively and at the same time, provide an easy way for data subjects to verify their details and request for any corrections or deletion of data.

4.2 Processing of Election Data

Entities processing election data need to show the basis for processing personal data. The Data Protection Act provides the circumstances under which data should be processed. Further, the Guidelines Note provides for specific circumstances which could affect the processing of election data including: compliance with any legal obligation to which the controller is subject, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, Consent.

Legal Obligation

Election stakeholders need to justify the exact law that confers a legal obligation to process personal data.

The Guidance Note states that an election stakeholder should be able to identify the obligation in question, either by reference to the specific legal provision or by pointing to an appropriate source of advice or guidance that sets it out clearly.[90]

Public Task

The Data Protection Act provides that a data controller or processor may collect and process data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[91]

The Guidance Note provides that the collection of data by the IEBC falls under this criteria given that the Election Act highlighted above mandates the IEBC to compile and maintain the Register of Voters, as part of its official authority, and may also collect "such information as the Commission shall prescribe".[92] Also the Guidelines states that the IEBC and other election stakeholders must justify which public task they are undertaking if they collect and process data not mandated by them under any written law.[93]

90. Guidance Note on Processing Personal Data for Electoral Purposes, s. 8
91. Data Protection Act 2019, s. 30
92. Election Act 2011, s. 4
93. Guidance Note on Processing Personal Data for Electoral Purposes, s. 8

Consent

Data collectors and processors are required under the Data Protection Act to obtain consent from data subjects prior to processing personal data. This ensures the collection and processing of data is: done lawfully, fairly and in a transparent manner; for the explicit, specified and legitimate purposes; and only where a valid explanation is provided whenever information relating to private affairs is required.

The Guidance Note states that consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. [94]

Further, data controllers or processors are prohibited from processing personal data, unless the data subject consents to the processing for one or more specified purposes.[95] The burden of proving or establishing that consent was properly obtained by the data subject falls on the data controllers and processors.[96]

The Guidance Note requires the IEBC to obtain the consent of the data subject prior to the collection of voters personal data since voters' personal and sensitive data is not a statutory right under the Election Act or a mandatory right.[97] However, statutory obligations will govern other aspects of the processing and use of the personal data.[98]

Likewise, political parties are required under the Guidance Note to obtain consent from their members before collecting the data for their own use and sharing it with the Registrar of political parties for verification and publication.[99] Currently the IEBC and political parties do not have policies that indicate how they obtain consent prior to their collection and processing of voters data. In addition, they have not provided details of what measures they have taken to ensure that consent is properly obtained from data subjects.

With respect to election campaigns, the Data Protection Act requires data controllers and processors not to use a data subject's data for commercial purposes, unless direct consent is obtained from the subject.[100] Therefore, in order to conduct political advertising, political parties are required to obtain consent from data subjects to use their data to send them political messages.[101] The Guidance Note states that where voters are subject to automated decision making processes such as to receive political advertising, they have the right to be informed by the political parties why they are receiving such adverts.

Further, under the Data Protection (General) Regulations direct marketing is classified as displaying an advertisement on an online media site a data subject is logged on using their personal data, including data collected by cookies, relating to a website the data subject has viewed; or sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.[103] Therefore, if political

94. Ibid
95. Ibid, s.30
96. Ibid, s. 32
97. Guidance Note on Processing Personal Data for Electoral Purposes, s. 8
98. Ibid
99. Ibid
100. Data Protection Act, s. 37
101. Guidance Note on Processing Personal Data for Electoral Purposes, s.10
102. Ibid
103. Proposed Data Protection (General) Regulations 2021, s. 13

parties display or send messages in the ways indicated in the definition, it will be classified as political advertising for which consent should be sought.

4.3 Sensitive Personal Data

The Elections Act requires the use of a biometric system for voter registration, and the Data Protection Act classifies biometric data as sensitive personal data.[104] Section 44 of the Data Protection Act requires that sensitive data is collected and processed in a manner compatible with the principle of data collection.[105]

Further, section 45 of the Act requires that the data is processed only for the establishment, exercise or defence of a legal claim; the purpose of carrying out the obligations and exercising specific rights of the controller.[106] Further the Guidance Note states that the processing should comply with the principles of data protection.[107] Moreover, any election stakeholder processing personal data will need to prove the lawful basis they are using to process the data.[108]

In light of the foregoing, the election laws should be reviewed and amended to be in line with the Data Protection Act. Moreover, the IEBC can only collect and process biometric data to carry out the election. The data should not be misused or shared with other entities for any other purpose. Thus, as it conducts voter registration, the IEBC needs to ensure that they adhere to the Data Protection Act in collecting the sensitive data. Further, whereas the election regulations allow individuals to request data from the IEBC, the IEBC should not share sensitive personal data such as biometric data. Biometric data should only be accessible if requested by the data subject.[109]

4.4 Obligations of Data Controllers and Processors

Under the Data Protection Act, the IEBC and political parties are required to inform the data subject of their rights when collecting and processing data; the fact that personal data is being collected; the purpose of which the data is being collected; third parties which they will share the data with; and a brief description of the security measures that they have taken to ensure that the data is safe.[110]

The collection and processing of data will mainly occur during the process of voter and candidate registration, nomination, campaign, voting and verification of results.

Data subjects should also be aware of their rights under the Data Protection Act. These include the right to: be informed how their data will be used; access their data held by the bodies; object on reasonable grounds the processing of their data; the correction of false or misleading data held by the data controller and processor; and the deletion of false and misleading data about them regarding their voting information.[111]

However, the Guidance Note states that the right to object is limited when processing is required for the performance of a public task (such as maintaining the voter register or publishing of a member register).[112] For example, a data subject can object to the processing of their email or telephone contact details but not to the use of their name, identification, address or such other personal data as the Commission deems necessary, within reason, for the purpose of maintaining and publishing the Register of Voters, if the data subject is a registered voter.[113]

104. Data Protection Act, s. 2
105. Ibid, s. 44
106. Ibid, s. 45
107. Guidance Note on Processing Personal Data for Electoral Purposes, s. 8.5
108. Ibid
109. Data Protection Act, s.26
110. Ibid, s. 29
111. Ibid, s.26
112. Guidance Note on Processing Personal Data for Electoral Purposes s. 10
113. Ibid

Further, the Guidance Note states data subjects have the rights to request political parties to rectify or delete any data they have on them and object to their data being processed for political advertising purposes. In addition, the right to erasure does not apply to data collected for carrying out a public task.

This includes the maintenance of Register of Voters by the IEBC or public member register by the Registrar or where it is necessary for archival in the public interest.[114] However, data subjects can request for certain aspects of their data to be erased such as contact information which is not required for maintenance of the register.[115]

The IEBC is obliged to incorporate data protection in their voter education training manuals and in their awareness campaigns. As has been witnessed during the 2022 mass voter registration exercise, the Commission does not inform data subjects of their rights and reasons why they are collecting the data. Further, the Guidance Note states that election stakeholders should develop privacy notices that inform the data subject of their rights under the Data Protection Act.[116] The notices should be in a clear plain language and be provided free of charge and should also be updated regularly. This research has also established that the Commission does not have a data protection policy placed on its official website.

4.5 Data Protection Impact Assessment

At the planning and implementation stage of the election cycle entities such as the IEBC, the Office of the Registrar of Political Parties, telecommunication companies and political parties should conduct data protection impact assessments (DPIA).

This is because election data falls under processing that may result in putting at risk the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes as stated in the Data Protection Act.[117] Also, the IEBC is under obligation to conduct a data impact assessment test on the system they will procure to safeguard the data they collect and process.

The importance of conducting a DPIA was highlighted by the High Court in October 2021 where it ruled that the government should have conducted a DPIA before proceeding to issue the Huduma Cards.[118] The court also found that the Data Protection Act applied retrospectively. The implication of this judgement to election stakeholders is that it will behoves them to review their data collection and processing activities and ensure they are in line with the Data Protection Act. The IEBC and other key election stakeholders such as political parties have not publicly stated whether they have conducted DPIA, and it remains to be seen the measures the ODPC will take to ensure compliance with the data protection laws.

114. Ibid
115. Ibid
116. Guidance Note on Processing Personal Data for Electoral Purposes, s. 9
117. Data Protection Act 2019, s. 31
118. Judicial Review Application Number E1138 of 2020, http://kenyalaw.org/caselaw/cases/view/220495/

5 Conclusion & Recommendations

This section presents the key conclusions and highlights the recommendations to various stakeholders including the Independent Electoral and Boundaries Commission (IEBC), Office of the Data Protection Commissioner (ODPC), Political Parties, Private Sector and Civil Society.

5.1 Conclusion

This brief has highlighted several challenges that threaten the right to privacy and the protection of personal data during an election context. Some of these include the gaps in the legal frameworks, low awareness and compliance of processes with standards set in the data protection laws, violations of data subjects' rights, and low awareness of data privacy rights.

The upcoming 2022 election presents a useful testing ground to assess the effectiveness of the Data Protection Act and the capacity of the ODPC to effectively enforce the law, especially given its internal capacity gaps such as staffing and funding.

Guaranteeing the respect for the right to privacy and the protection of personal data in an election context will require the review of the various laws, policies, regulations, systems and practices to comply with the standards set under the Data Protection Act. It will also call for greater investment of all election stakeholders, to ensure an enabling environment for the protection and promotion of the right to privacy during the entire election cycle.

5.2 Recommendations

The IEBC should:

a) Review all internal processes relating to the voters' data and ensure compliance with the Data Protection Act.

b) Develop comprehensive data protection policies and notices.

c) Propose updates to the IEBC Elections (Technology) Regulations, 2017 to accommodate the provisions of the Data Protection Act.

d) Ensure the Kenya Integrated Election Management System (KIEMS) incorporates the principles of privacy by design and default.

e) Review the voter education manual to incorporate privacy aspects.

f) Educate and inform voters of their rights under the Data Protection Act.

g) Train election officials on how to ensure privacy and data protection of voters' personal data.

h) Conduct a Data Protection Impact Assessments and Data audits.

The Office of the Data Protection Commissioner should:

a) Oversee the data collection and processing operations of the various election management bodies to ensure compliance with the Data Protection Act.
b) Assess and inspect the systems used by the key election stakeholders to ensure that they comply with the Data Protection Act.
c) Collaborate with the IEBC, ORPP, political parties and other election stakeholders to create awareness of privacy and develop a code of practice for the use of personal data in political campaigning, such as has been developed by the UK's Information Commissioner's Office.[119]
d) Create awareness on privacy and data protection during an election context.
e) Facilitate the reporting of misuse of personal data by data controllers and processors.
f) Conduct timely investigations of complaints of data misuse.

Political Parties should:

a) Adhere to the Data Protection Act when handling personal data of members.
b) Review all internal processes relating to the voters' data and ensure compliance with the Data Protection Act.
c) Develop comprehensive data protection policies and notices.
d) Train party officials on how to ensure privacy and data protection of voters' personal data.
e) Inform data subjects of the collection and processing of their data and the purpose of the collection.

Private Sector (Telecommunication and Social Media Companies) should:

a) Ensure their systems used during the election are privacy respecting and secure by design.
b) Conduct regular independent cyber threat tests on their systems supporting the elections.
c) Actively monitor incidents of misinformation and data scraping by political parties to use the data for political advertising.
d) Adopt rigorous measures to enable users to block spam messages and stem the abuse of their personal data by political parties and other groups sending unsolicited short messages and targeted political messages.

Civil Society should:

a) Educate the public to cultivate a value system that promotes privacy and data protection in the election process.
b) Create awareness on privacy rights, including the means to report any violation of privacy rights and the misuse of personal data breaches during the election process to the ODPC.
c) Monitor the privacy and data protection environment, including the practices of data controllers and processes, and highlight any malpractice to the ODPC.
d) Build partnerships with other election stakeholders to promote respect for privacy and data protection.

119. Guide for the use of personal data in political campaigning https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/

www.kictanet.or.ke