CONTEXTUALISING POLITICAL ADVERTISING POLICY TO POLITICAL MICRO-TARGETING IN KENYAN ELECTIONS

Joshua Kitili ▪ Joseph Gitonga Theuri ▪ Khalil Badbess

Strathmore University

Centre for Intellectual Property and Information Technology Law

TABLE OF CONTENTS

A. INTRODUCTION

Technological advancements have significantly impacted the political world. Unlike the traditional means of conducting campaigns, technology makes it possible to conduct data driven campaigns on a large scale and with high levels of specificity. On account of the increased use of digital tools and digital channels of communication, individuals are now leaving behind digital footprints with vast amounts of data that can be used to make inferences about an individual or group.[1] For political parties, better clarity leads to hyper-individualised communication in a process known as micro-targeting.[2]

The practice of political micro-targeting, although not new, has grown in scale in recent years and attracted a great deal of attention for two reasons: the emergence of social media as a communication channel and the existence of big data.[3] Micro-targeting is a multi-step process that commences with the collection of data to analyse it with the aim of understanding people's behaviour and opinions.[4] The collection of data is followed by a categorisation of individuals based on their inclinations such as similar concerns and opinions over issues.[5] Political microtargeting often involves analysis of large data sets and use of predictive modelling that matches an individual's personal preferences with their political beliefs so as to produce a desired voting decision from that individual.[6] Targeted personalised messages by political actors are later disseminated to the relevant audience.[7]

Micro-targeting has attracted its fair share of criticism due to its recorded harmful effects on individual privacy and the democratic values of a country.[8] For example, the ruling party in India uses 'in-depth demographic profiles to target voters based on caste or religious demographics.'[9] The microtargeting practice in India is often reliant on misinformation and hateful rhetoric and has a harmful effect on the democratic public discourse.[10] However, as there is little data on the different applications of data in a campaign it is difficult to determine the extent of a data driven campaign and whether it is problematic.[11] While the true impact of micro-targeting is yet to be seen[12] in many countries other than a few that have been documented in the recent past-yet, we argue

[1]IDEA,*Digital Microtargeting*(19 June 2018)<https://www.idea.int/publications/catalogue/digital-microtargeting> accessed 1 July 2022

[2]ibid

[3]Orestis Papakyriakopoulos and others, *Social media and microtargeting: Political data processing and the consequences for Germany* < https://journals.sagepub.com/doi/pdf/10.1177/2053951718811844 > accessed 1 July 2022

[4]Frederik J. Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy'(2018) 14 (1) Utrecht Law Review 82-96

[5]ibid

[6]Ira S.Rubinstein, 'Voter privacy in the age of big data' < https://deliverypdf.ssrn.com/delivery.php? ID=673064096005020112031018111100031100001024071012061053073118019088121006070114102091011099101107042108110073127022077102088100031034078007004030960050211041220380470370130181170041081060061140990671010000310990750090081030671201191040720971150 04&EXT= pdf&INDEX=TRUE > accessed 1 July 2022

[7]Borgesius (n 4)

[9]The Guardian, *Leaked: Cambridge Analytica's blueprint for Trump victory* <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory > accessed 1 July 2022

[10]ibid

that its effects should not be understated. Although the practice has a number of benefits, the threats it poses outweigh the benefits; primarily due to the threat it poses to individual privacy and its potential to suppress voter population.[13] Individual privacy threats include data breaches of the personal data and also misuse of voters' personal data.[14]

This study will primarily focus on microtargeting and not disinformation. Disinformation is mainly concerned with the intentional dissemination of misleading and wrongful information which seeks to 'shape perceptions around some aspect of political discourse'[15] whereas microtargeting involves the use of predictive modelling to produce a desired voting decision.

The study employs a multi-phase approach in the study of microtargeting in Kenya's political landscape. In the first phase, the study analyses paid Facebook advertisements for political candidates who participated in the 2022 nationwide presidential elections and the gubernatorial elections held in each of Kenya's 47 counties to determine the type and extent, if any, of political micro-targeted ads deployed in each of the two election cycles. In the second phase, the study employs the doctrinal research approach in assessing existing laws applicable to microtargeting in Kenya; identifying gaps in the laws that allow or justify specialised online advertising regulations, and analysing existing external regulatory initiatives that Kenya can borrow from which will aid in formulating a comprehensive law to regulate political microtargeting.

Objectives of the study

The objectives of the study were as follows,

i. To determine the advertising tools available to political actors on Facebook that might enable political micro-targeting during the 2022 Kenyan presidential and gubernatorial election campaigns.

ii. To infer the targeting criteria in political advertisements on Facebook by political actors involved in the 2022 Kenya general election campaigns.

iii. To determine the type and extent of political micro-targeted ads deployed.

iv. To investigate whether online political advertising regulations in Kenya can be designed to restrict and detect online political micro-targeting practices that infringe on Kenyans' rights to privacy and meaningful political participation.

v. To determine the laws applicable to political microtargeting in Kenya.

vi. To analyse the shortcomings or gaps in the Kenyan laws that are applicable to political microtargeting and make appropriate recommendations.

vii. To contextualise external policy initiatives on political advertising to Kenya and consider their effectiveness in the country's context.

[11] Jessica Baldwin-Philippi, *The Myths of Data-Driven Campaigning* < https://www.tandfonline.com/doi/abs/10.1080/10584609.2017.1372999?journalCode=upcp20 >accessed 1 July 2022

[12] Balazs Bodo, Natali Helberger and Claes H.de Vreese,'Political micro-targeting: a Manchurian candidate or just a dark horse?'(2017) 6(4)Internet Policy Review 1-13

[13] Agniete Pocyte, *Online Political Microtargeting in the United States* < https://thesecuritydistillery.org/all-articles/online-political-microtargeting-in-the-united-states > accessed 7 September 2022

[14] Borgesius (n 4)

[15] ICNL, *Disinformation: The Legislative Dilemma* <https://www.icnl.org/wp-content/uploads/Disinformation-The-Legislative-Dilemma..pdf > accessed 20 September 2022

B. METHODOLOGY

In the first phase, data collection focused on paid Facebook advertisements for political candidates that took part in the 2022 presidential and gubernatorial elections held in each of the 47 counties in Kenya. The purpose was to determine the type and extent if any, of political microtargeting ads deployed. Instead of creating a developer account, the public version of the ad archive on Facebook was used so as to enable the collection of ad information. The data obtained determined the specificity of political microtargeting taking place through these ads based on the targeting criteria and advertising tools used by relevant actors.

For the second phase, analysis of the legal protections offered in Kenya's electoral process as it concerns micro-targeted advertisements, data regarding political microtargeting in Kenya was collected through desktop research. Secondary sources expounding the state of political micro-targeting in Kenya, the existing legal framework and its shortcomings were analysed and the findings deduced. Doctrinal research was used to analyse secondary data specifically the existing Kenyan laws applicable to political microtargeting. In proposing online political advertising regulation to supplement existing laws, the comparative research method was employed by assessing policy initiatives from other countries and obtaining data from multiple jurisdictions which were ideal in making regulatory and policy recommendations.

Picture by Rohan Odhiambo https://unsplash.com/photos/rLjWNCr84VA

C. LITERATURE REVIEW

In the aftermath of the Facebook/Cambridge Analytica scandal, there is now global attention to the different ways that personal data is processed in election campaigns. Elections have to some extent and with enormous variations, become "data-driven."[16] The categorization and profiling of precise groups of voters has arguably facilitated "political microtargeting" through an international political "influence industry."

Although political micro-targeting is now assumed to be widespread among Western democracies, some contend that the phenomenon is poorly understood. There are, some commentators who regard the term as inherently misleading, and essentially indistinguishable from the behavioural advertising tactics used for general consumer marketing.[17] There is also increasing scepticism about whether political micro-targeting is that effective. Popular writing about these technologies, as well as the corporate hype, typically oversells the impact of these practices. There is plenty of mythology surrounding data-driven campaigns, and evidence that these techniques are far more effective at mobilizing adherents than in persuading voters to change their attitudes and behaviour.[18]

In this study we investigate micro-targeting in the 2022 Kenya General Election. Employing the Facebook political advertising public archive, we investigate a range of digital ads delivered by different parties and candidates at different stages in the election campaign. We are not so much interested in whether the ads were negative or positive, a topic of extensive and historical interest,[19] nor are we interested in the question of whether the ads are true or false. Again, there is a growing literature on false advertising and the viral spread of "disinformation" and its various effects on democratic values and institutions.[20]

Although our research holds lessons for the appropriate level of transparency of digital political advertising, and for the practices of platforms like Facebook in the future, that is not the main aim. Rather, we are more interested in how mainstream political parties in Kenya use the medium. How do they advertise? To whom, when, and how? In reality, how much micro-targeting did the typical voter actually see in the recent general election? Only when we understand the scale and nature of the practice, can we begin to assess the "macro-effects" of micro-targeting[21] and the normative implications for Kenyan democracy.

[16]Colin J. Bennett and David Lyon, 'Data-driven elections: implications and challenges for democratic societies' (2019) 8 (4) Internet Policy Review 1- 16
[17]Jeff Chester and Kathryn C. Montgomery, 'The digital commercialisation of US politics-2020 and beyond' (2019) 8 (4) Internet Policy Review 1 -23
[18]Jessica Baldwin-Philippi, ' Data campaigning: between empirics and assumptions' (2019) 8(4) Internet Policy Review 1-18
[19]Donald Green, *Do Negative Political Ads Work?* (1 September 2013) < https://www.scientificamerican.com/article/do-negative-political-ads-work/ > accessed 21 September 2022
[20]Bennett, W. Lance and Steven Livingston, 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions' (2018) 33 (2) European Journal of Communication 122-139
[21]Stephanie Hankey, Julianne Kerr Morrison and Ravi Naik, *Data and Democracy in the Digital Age* < https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf > accessed 21 September 2022

Micro-Targeting and Macro-Effects

There has probably been greater attention to the macro-effects of micro-targeting than to the nature and extent of the practice itself. There are, of course, significant concerns about the "consumerization of the political space" and huge implications of treating voters like consumers -- or "shopping for votes."[22] There have also been profound concerns about divisiveness and the question of whether micro-targeting leads to an increased tendency to deliver messages on "wedge issues."[23] Micro-targeting may also hold the danger of "filter bubbles" or "echo chambers" when individuals only see a subset of information algorithmically curated according to their presumed and prior interests and behaviours,[24] producing broader concerns about the effect on the "marketplace of ideas" when false advertising cannot be countered in real-time. In the open, false claims might be challenged; in secret, they may stand unchallenged.

There are also possible effects on political participation and engagement. Does the precise segmentation reduce the portion of the electorate that politicians need to campaign to and for, and ultimately care about after the election? Are the interests of others then ignored, or marginalized? More widely, does micro-targeting contribute to a decline in political participation, as voters perceive that their interests are being manipulated by political and technical elites? Do data-driven elections discourage volunteering for political parties? Do data-driven elections favour larger and more established political parties, which have the resources to employ the technical consultants to manage the data and coordinate the messaging?[25]

The answer to these, and other, questions about micro-targeting depends of course on how micro-targeting is defined, as well as on the granularity of the advertising in any one election. In general terms, micro-targeting is a concept used to distinguish modern forms of targeted advertising from the broadcasting model prevalent in the past, where the same message is delivered to everyone regardless of location, demographic characteristics, or policy preferences.[26]

It is impossible to pinpoint an exact point at which consumer micro-targeting techniques entered the political arena, although the 2004 presidential campaign of George W. Bush is often regarded as a watershed moment. Subsequently, the observation of the skilled way that data analytics was employed in the two elections won by Barack Obama in 2008 and 2012 then led to a general assumption that campaigns in the U.S. needed, to some extent, to be data-driven to be successful. That assumption soon spread to other countries and a general desire to use data analytics to gain an edge over their rivals.[27]

Micro-targeting is conducted across a number of different dimensions and variables. The practice varies along a continuum with the mythical "unified view" of the voter at one extreme end, and the mass general messaging to the entire population at the other. Most "micro-targeted" messages, therefore, fall somewhere in between and are more or less "micro" depending on location, target audience, policy message, and means of communication. Thus, micro-targeted messages might be directed towards a precise demographic in many constituencies. But they may equally be directed towards a broader demographic within a more precise location. A precise and localized policy promise, for instance, might appeal to a very broad population within a specific region.

---

[22]Susan Delacourt, *Shopping for Votes: How Politicians Choose Us and We Choose Them* (Douglas & McIntyre 2013)

[23]D. Sunshine HIllyGus and Todd G. Shields, *The Persuadable Voter: Wedge Issues in Presidential Campaigns* (Princeton University Press 2008)

[24]Eli Pariser, *The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think* (Penguin Publishing Group 2012)

[25]Colin J. Bennett and David Lyon, 'Data-driven elections: implications and challenges for democratic societies' (2019) 8 (4) Internet Policy Review 1- 16

[26]Kyle Endres and Kristin J. Kelly, 'Does microtargeting matter? Campaign Contact Strategies and Young Voters' (2017) 28 (1) Journal of Elections, Public Opinion and Parties 1-18

[27]Colin J. Bennett, *The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies* (15 June 2013) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2279920 > accessed 21 September 2022

Furthermore, micro-targeting will only be as good as the modelling that drives the algorithms.[28] If the assumptions about the electorate are incorrect, then the messaging will also be redundant. It is also presumed, in much of the recent literature, that micro-targeted messages are associated predominantly with Facebook. This is not necessarily true; micro-targeting might find audiences through many means of communication – e-mail, text, phone, as well as paper leaflets and signage. The effective message in an election campaign must account for content, audience, timing, and means (the what, who, when, and how)

State of Political Microtargeting in Kenya

In Kenya, a former executive to a British data analytics firm is on record stating that they rebranded a well-known party in the country twice, wrote their manifesto and did research and analysis. [29] The data analytics firm is quoted as having said that the surveys conducted covered 'key national and local political issues, levels of trust in key politicians, voting behaviours/intentions, and preferred information channels'.[30] As a result, the company described its operations for the 2013 elections as 'the largest political research project ever conducted in East Africa' and further admitted to using tribal divisions in its political messaging.[31]

The firm is suspected to have used the large-scale data gathered from the aforementioned surveys, Kenya's publicly available voter registration databases and the data it collected from Facebook to conduct online political micro-targeting on digital platforms to sway voters' decisions.[32] To provide an example, with the requisite data, advertising options on a platform like Facebook can be used to micro-target voters during elections. Some of the ways in which audiences can be segmented and micro-targeted on Facebook are through advertising tools like 'custom audiences' and 'look-alike audiences'.[33] Custom audiences allows advertisers to create audience segments that they want to include or exclude in paid political advertisements.[34] In doing so, political actors can 'upload the voter file they have purchased and match other information they have about you to your voting history.[35]

Look-alike audiences allows 'advertisers to upload a list or select a custom audience of people and then, using a complex algorithm, create an audience that is likely to be just as receptive to the messaging as the initial custom audience.[36] Presumably, tools like this built on the psychographic profiles that the firm built from the data it collected.

[28]Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)

[29]BBC, *Cambridge Analytica's Kenya election role 'must be investigated'*< https://www.bbc.com/news/world-africa-43471707 > accessed 1 July 2022

[30]ibid.

[31]Justina Crabtree, *Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections*<https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html > accessed 1 July 2022

[32]Abdulmalik Sugow A and Isaac Rutenberg, *Securing Kenya's Electoral Integrity: Regulating Personal Data Use* (1 October 2021)< https://www.theelephant.info/op-eds/2021/10/01/securing-kenyas-electoral-integrity-regulating-personal-data-use/ > accessed 1 July 2022

[33]Meta, *How to Use Custom or Lookalike Audiences*<https://www.facebook.com/business/help/572787736078838?id=176276233019487 > accessed 1 July 2022

[34]Kaili Lambe and Becca Ricks,*The basics on microtargeting and political ads on Facebook* <https://foundation.mozilla.org/en/blog/basics-microtargeting-and-political-ads-facebook/ > accessed 1 July 2022

[35]ibid

[36]ibid

Political Microtargeting Threats on Kenyan Citizens

Invasion of Privacy

Since online political microtargeting involves gathering and combining people's personal data on a massive scale to identify political preferences, the data gathered threatens the privacy of individuals. For instance, if people are suspicious that the websites they visit are being tracked, they may not be comfortable to visit certain websites. Also, by tracking people's use of the internet, a company can come up with a 'database of individuals and their interests.[37] An example of invasion of privacy is what happened in 2011 in Ireland when there was interference of Fine Gael's website by denial of service attacks that resulted in personal details of up to 2000 users of the site being compromised.[38]

Data Breaches

Data is prone to cybercrime offences especially if adequate measures are not taken to protect it. Offences where the computer is the target can interfere with data that is already in the computer. The conduct which these offences seek to address include:

i. The gaining of unauthorised access to a computer or computer system.[39]

ii. Causing unauthorised damage to computer data.[40]

iii. The unauthorised interception of computer data.[41]

Where personal data has been collected for microtargeting purposes and adequate measures have not been put in place to protect the data, hackers or others can access databases containing the personal data and misuse it. For example in 2017 the U.S Republican Party contracted a marketing company which suffered a data breach thus exposing the personal data belonging to almost 200 million US citizens.[42]

Misuse of personal data

The personal data collected for microtargeting purposes can be used for other purposes which can even be harmful thus threatening the privacy of individuals. For example in Brazil, marketing firms were hired by political parties to develop a data driven campaign for WhatsApp and other platforms. The marketing firms used great amounts of user data including identification information such as location and age for purposes of 'disseminating news, misinformation and propaganda through the various social media channels.'[43]

Manipulation of voters

A party could use 'tailored information that maximises or minimises voter engagement.'[44] The targeted information can be false and still have maximum impact. Gorton warns that microtargeting facilitates the spread of misinformation.[45] Cambridge Analytica is a good example because it has often been accused of overselling its capabilities in the elections that it participated in.[46]

---

[37]Frederik J. Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy'(2018) 14 (1) Utrecht Law Review 82-96

[38]Colin J. Bennett, 'Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North Armerica? (2016) 6 (4) International Data Privacy Law 261-275

[39]Jonathan Clough,*Principles of Cybercrime* (Cambridge University Press 2010)

[40]ibid

[41]ibid

[42]Borgesius (n 37)

[43]accessnow, *Your data used against you: reports of manipulation on WhatsApp ahead of Brazil's election* <https://www.accessnow.org/your-data-used-against-you-reports-of-manipulation-on-whatsapp-ahead-of-brazils-election/ > accessed 20 September 2022

[44]Borgesius (n 37) 87

[45]ibid

[46]Angela Chen and Alessandra Potenza, *Cambridge Analytica's Facebook Data Abuse Shouldn't get credit for Trump*(20 March 2018)<https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting > accessed 20 July 2022

In particular, Analytica's claim that it could sway voters' decisions by sending targeted messages attuned to their psychological profiles has been scrutinised.[47] The nexus between psychological profiling and political micro-targeting on voter decision-making is thought to be inadequately proven by existing research.[48] This is not to say that targeted advertising based on psychological characteristics is generally ineffective. In a relatively recent study, Matz, Kosinski, Nave, and Stillwell demonstrated that designing Facebook advertisements based on psychological factors 'resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or impersonalized counterparts'.[49] Moreover, it has been argued that influencing political behaviour through psychographic profiling and micro-targeting might be drastically different from the consumer decision-making context studied by Kosinski et al.[50]

Despite these limitations, one may still ethically condemn aspects of political micro-targeting not necessarily based on its efficacy but on the principle and ends for which it is conducted. If, for example, an instance of political micro-targeting seeks to psychologically manipulate voters, even if it does not achieve this goal, then that instance of micro-targeting would principally be wrong. Furthermore, data-driven campaigning technology has evolved remarkably in the last few years and thus the efficacy with which psychographic profiling and political micro-targeting affect voter decision-making might also improve.

Voter exclusion

Microtargeting can be used by political parties to exclude certain voter groups. Some groups of voters can be ignored during the campaign season because a political party 'does not expect them to vote'[51] or it has high expectations of winning elsewhere. Also, certain voters who are deemed not likely to vote can be excluded from receiving political messaging, essentially exempting them from meaningful political discussion.[52]

[47]ibid.

[48]ibid.

[49]Matz S, Kosinski M,Nave G and Stillwell D, 'Psychological targeting as an effective approach to digital mass persuasion' (2017) 114(48) PNAS 12714-12719.

[50]Chen (n 46)

[51]Borgesius, F. J. Z., Möller, J., Kruikemeier, S., Fathaigh, R. Ó., Irion, K., Dobber, T., ... & De Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82-96.

[52]William Gorton, 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy'(2016) 38(1) New Political Science 61-80

D. COMPUTATIONAL ANALYSIS

The extent of microtargeting in Kenya's electoral process is a contentious issue. In an effort to gain a clearer understanding of its role in the Kenya's elections, an analysis of the political advertisements on Facebook during the official campaign period in the 2022 Kenyan elections was carried out. Facebook was selected as the platform of study because of the high percentage of Kenyan citizens that utilize the platform. As of March 2022, 12 million Kenyans used the platform and Facebook's ad reach in Kenya was equivalent to 17.9 percent of the total population.[53]

Determining Political Micro-Targeting on Facebook in Kenya's 2022 elections

This technical study examines paid Facebook advertisements for political candidates who participated in the 2022 general election to determine the type and extent, if any, of political micro-targeted ads deployed. The big question is - was there "micro-targeting" going on? If so, how much and with what level of precision? In this study we consider not only the precision of the audience in demographic or geographic terms, but also the theme surrounding the message itself. In doing so the focus is made not just on the who, when, and how, but also the what -- the nature of the message. This contends that a micro-targeted message should contain a focused location, a precise demographic, and critically a focused theme.

Political Micro-Targeting on Facebook

The Facebook ads platform provides three approaches for advertisers to target people,

i. ***Personally Identifiable Information (PII)*** targeting is the form in which advertisers provide personal information about users such as name, phone number, and email address so that Facebook can directly place the ads to them. This option is useful if a candidate already has a list of supporters. These lists may be composed of known supporters of the political party or could be derived by an individual signing a petition, or liking the group on Facebook.

ii. ***Look-alike audience target*** is the targeting option in which advertisers provide to Facebook a list of users similar to that one in the PII or a list of people who liked the advertiser Facebook page. Then, Facebook attempt to target a similar audience to the group in this specific list.

iii. ***Attribute-based targeting*** allows the advertiser to create a target formula based on a wide range of elements that include user basic demographics (i.e., gender, age, location, language), advanced demographics (i.e., political leaning, income level, 'Parents with children pre-schoolers'), interests (i.e., newspapers, religion, politics), and behaviours (i.e. 'Business Travellers' or 'New Vehicle buyers').

[53]Simon Kemp, "Digital Kenya:2022", https://datareportal.com/reports/digital-2022-kenya

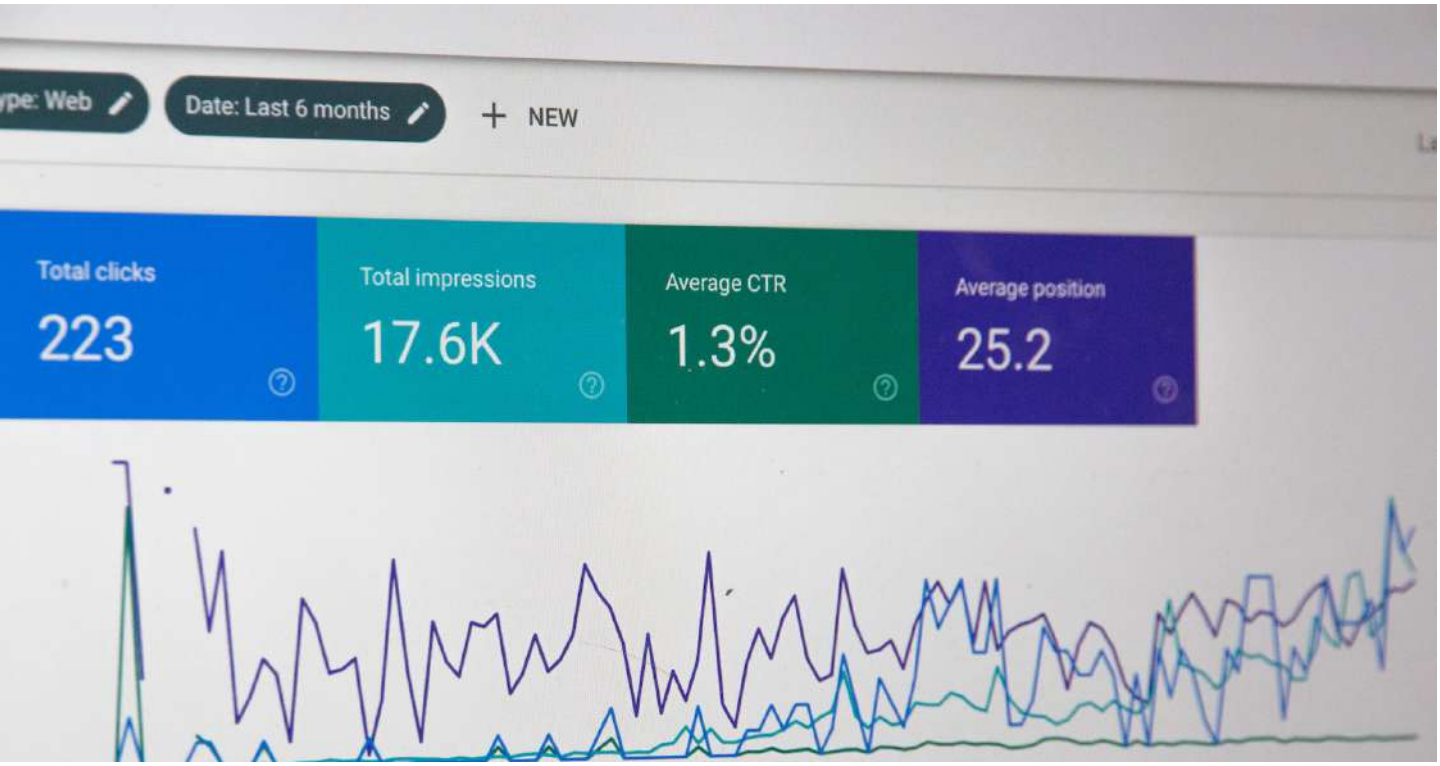
Facebook Data Collection

Facebook provides two ways to access its ad archive. The first involves the creation of a developer account on Facebook, contingent on application and identity verification. Once this has occurred, information can be queried by one of the following fields (Ad Library API, n.d.)[54] start and end date when the ad ran, the ad copy, the "ad creative", which you can view at a given URL, the currency used to pay for the ad, the ad funding entity, the Facebook Page ID for the Page that ran the ad, and ad performance data including the rough amount spent, rough impressions, and the demographic distribution, (according to age, gender, and location) as a percentage of total audience reached. Facebook has also developed a social media analytics tool known as Crowdtangle which is used to track posts on public accounts, pages and groups.[55]

Facebook also reports the number of "impressions" for each ad. Facebook defines impressions as the "total number of times the ad referenced has been shown on the site."[56] Thus, when an ad appears on the right side of the screen while a user is viewing Facebook, an impression is registered to that Facebook account. This metric is distinct from the number of times the ad is clicked on. If we do not understand how the audience was developed, we cannot state whether it is or is not a form of micro-targeting.

Rather than creating a developer account, or install a browser plug-in, we used the public version of the ad archive. This version provides a grid-style list of advertisements that can be queried based on a keyword or page search. Additionally, the ad archive filters search results by country, whether the ad is currently active and being displayed to users or inactive (archived), the number of impressions, whether the ad had a political disclaimer, and the platform on which the advertisement was displayed; Facebook, Audience Network (Facebook ads delivered outside of Facebook), Messenger, or Instagram. The advertisement image and message are displayed alongside additional information such as the ad ID, date range of when the ad was active, who paid for the advertisement, a rough range of how much was spent on it, a rough range of how many people saw the

Picture by Stephen Phillips https://unsplash.com/photos/shr_Xn8S8QU



[54] *Ad Library API*. (n.d.). Retrieved September 20, 2022, from https://www.facebook.com/ads/library/api
[55] https://www.crowdtangle.com/
[56] "In the Old Reports, What Do the Terms in My Exported Advertising Performance Report Mean? | Facebook Help Center," accessed October 30, 2022, https://www.facebook.com/help/213861005301603.

advertisement, what province(s) the ad was displayed in, and the age range and gender of the people who saw this ad.

The collection period selected began from May 29th 2022[57] (the official campaign kick-off date) and ended one day before the General election, 8th August 2022. In total the dataset comprised of 3,319 Facebook ads.

Design Framework

The Facebook archive permits a basic assessment of the variations in micro-targeting across three broad variables: the specificity of the policy message; the narrowness or breadth of the demographic (age and gender); and the precision of locational targeting. Those different combinations yield eight different levels of messaging. We use this framework to try to discern the patterns of Facebook advertising, and also to question the kinds of political micro-targeting observed.

We also make no distinction in our analysis between ads designed to persuade, and those designed to mobilize. A significant proportion of ads, especially, of course, those delivered in the last week of the campaign, had a quite basic Get-Out-the-Vote (GOTV) purpose, and we note these patterns below. We do not regard these as a separate category of micro-targeting, however. Even though GOTV messaging provides insights into electoral tactics, it adds little to our understanding of the extent and precision of micro-targeting.

3,319

number of facebook ads the dataset is comprised of.

Our interest is in discerning what the messages actually look like to the voters targeted. Given these constraints, do these messages look like micro-targeting? Do they cross a threshold of intrusiveness? With these qualifications, we now examine each category of targeting in turn and attempt to discern whether we see any clear patterns across the political spectrum.

Text Classification

In order to extract the demographic (age and gender) and geographic (region) classification labels a statistical significance test on the proportion data provided by Facebook was conducted. The upper tailed t-test is considered in order to check the significance of the hypothesis H_1: $\mu > \mu_0$, where μ is the mean. In other words, we seek to identify which group among the features had significantly more focus than others.

Since our detection is in charge of distribution of Z_t values, a natural solution is to select the most anomalous confidence values in Z_0 relative to μ. Define

$$\Theta = t : t \in \{ \widehat{K}\widehat{K} + 1, \ldots, d\}$$

$$\text{s.t. } z_t \text{ is a targeted class relative to } Z_0,$$

so the anomalous confidence values are $\{z_t\}_{t\in\Theta}$. The result will thus be presented with $\{ (x_t, y_t)\}_{t\in\Theta}$ in the original domain of the data (class labels) as potential outliers. Additionally $|\Theta|$ may be restricted to be of maximal size, say 2; this is based on the ideas introduced in (Miller, 1956) that human short-term memory can handle only a limited number of items. Not all of $\{(x_t, y_t)\}_{t\in\Theta}$ are a targeted class, but rather from selection at least one can be included (and at higher proportion than a random sample from $\{(x_t, y_t)\}$ $\widehat{K}\widehat{K} + 1 \leq t \leq d$). The goal is not

[57] "IEBC - Electionlaws," accessed October 30, 2022, https://www.iebc.or.ke/electionlaws/?Gazette_Notices.

to return most of the feature classes as outputs, but rather a few representative ones that help in diagnosis.[58]

The one sample t-test as a modified approach stemming from Duong is applied here.[59] The test takes as input a univariate samples (Z_0) and conducts a t-test estimate on each, denoted $\hat{f}\hat{f}_0$, a process which includes determining the optimal bandwidth values, which are inputs into the algorithm. The domain is discretized into n points $\{\delta_1, \ldots, \delta_n\}$. Let $\Delta i = \hat{f}\hat{f}_0(\delta_i) - \mu$. Assuming this discretization represents the densities well enough, a local test will be done at each δ_1 to see if the difference Δi is significantly different from μ. At each δ_1 the statistic

$$\chi^2_{stat}\chi^2_{stat} = \left(\frac{\Delta i}{\bar{SD}\ (\Delta i)}\right)^2\left(\frac{\Delta i}{\bar{SD}\ (\Delta i)}\right)^2$$

is calculated; the standard deviations of the differences Δ_i are obtained from a formula that relies on the density bandwidths. Each statistic is independently chi-squared $\chi_1^2\chi_1^2$ distributed. For each, the upper-tailed p-value is calculated; given a desired threshold $\alpha*$ yielding adjusted p-values $\{\pi_1, \ldots, \pi_n\}$, and thus a decision as to which δ_1 are locations of significant differences.

The individual tests are then used to determine significant classes. Let $\delta_a < \delta_b$ be two points in the discretization. An interval $[\delta_a, \delta_b] \in [0, 1]$ is an area where $\hat{f}\hat{f}_0$ and μ differ significantly if $\pi i < \alpha*$, $\forall a \leq i \leq b$, that is if there is a significant density difference at all intermediate discretization points δi. Let Λ be the union of all such intervals, if they exist. Thus, we define $\Theta = \{t : t \in \{\widehat{K}\widehat{K} + 1, \ldots, d\}\ \text{s.t.}\ zt \in \Lambda\}$, again restricted to a maximal size and choosing the intervals in Λ in order of the significance of their p-value given it is below $\alpha*$. The output is then given with $\{(x_t, y_t)\}_{t\in\Theta}$.[60]

Beyond this, to ascertain that the variance between the features is significantly different from the population variance further hypothesis testing is curried out to examine the deviation of each feature to its sample mean across different posts. The Gaussian (normal) distribution is most often assumed to describe the random variation that occurs in the data. However, the measurements show a skewed distribution. Skewed distributions are particularly common when mean values are low, variances large, and values cannot be negative, as was the case.[61]

Using the normal distribution where the log-normal is more appropriate can distort results derived from commonly used statistical tools. Linear statistical models, for example, assume that variability of the predicted variable is normally distributed. If, instead, it is log-normally distributed, then a log transform must be applied before the tool is used, or inferences based on the analysis may be biased. The inverse is also true; if a log transform is applied to data that really follows the normal distribution, then statistical analyses based on the transformed values will be misleading. Although the problem of model selection could be avoided by using nonparametric procedures, such as using Kruskal-Wallis instead of analysis of variance, those analyses are typically less powerful than comparable parametric ones when the data are normally distributed.

[58]Ackerman, S., Farchi, E., Raz, O., Zalmanovici, M., & Dube, P. (2020). Detection of data drift and outliers affecting machine learning model performance over time. *ArXiv Preprint ArXiv:2012.09258*.
[59]Duong, T. (2013). Local significant differences from nonparametric two-sample tests. *Journal of Nonparametric Statistics*, *25*(3), 635–645.
[60]Supra 31
[61]Limpert, E., Stahel, W. A., & Abbt, M. (2001). Log-normal distributions across the sciences: Keys and clues: on the charms of statistics, and how mechanical models resembling gambling machines offer a link to a handy way to characterize log-normal distributions, which can provide deeper insight into variability and probability—normal or log-normal: that is the question. *BioScience*, *51*(5), 341–352.

In this study, the impressions generated were fitted to the log-normal model to help lay a foundation for use of log-normal transforms used to normalize impressions before performing hypothesis testing.[62]

Topic Modelling

It is possible to categorize text documents using the information acquired from an unsupervised model, in this case, LDA. Latent Dirichlet Allocation (LDA) is a generative probabilistic model composed of a set of probabilistic mixtures that represent distributions over words. The appearance of a given word is conditioned to a set K of k topics, where each of these topics is defined by a set of keywords. The LDA model assumes that a probabilistic process generates a collection of M documents by sampling words from a dictionary of size V. This process goes as follows: for each of the M documents, the process starts by selecting a number of words N∼ Poisson(ξ), and a k-dimensional multinomial variable θ∼ Dir(α), which represents the influence of each topic in the document. Then, each word is randomly chosen by first selecting a topic zn∼ Multinomial(θ), and posteriorly, each word w_n is sampled from p(wn|zn, β), where β is a k × V multinomial distribution of words conditioned on the topics.[63]

All parameters can be obtained from a given corpus using different inference methods, such as variational Bayes approximation of the posterior distribution or sampling methods. Once all the parameters have been learnt, numerous information can be obtained.[64]

Picture by Stephen Dawson https://unsplash.com/photos/qwtCeJ5cLYs

[62]Strum, D. P., May, J. H., & Vargas, L. G. (2000). Modeling the uncertainty of surgical procedure times: Comparison of log-normal and normal models. *The Journal of the American Society of Anesthesiologists*, *92*(4), 1160–1167.
[63]Dorado, R., & Ratté, S. (2016). Semisupervised text classification using unsupervised topic information. *The Twenty-Ninth International Flairs Conference*.
[64] ibid 36

E. RESULTS

Analysing Target Audience Demographics

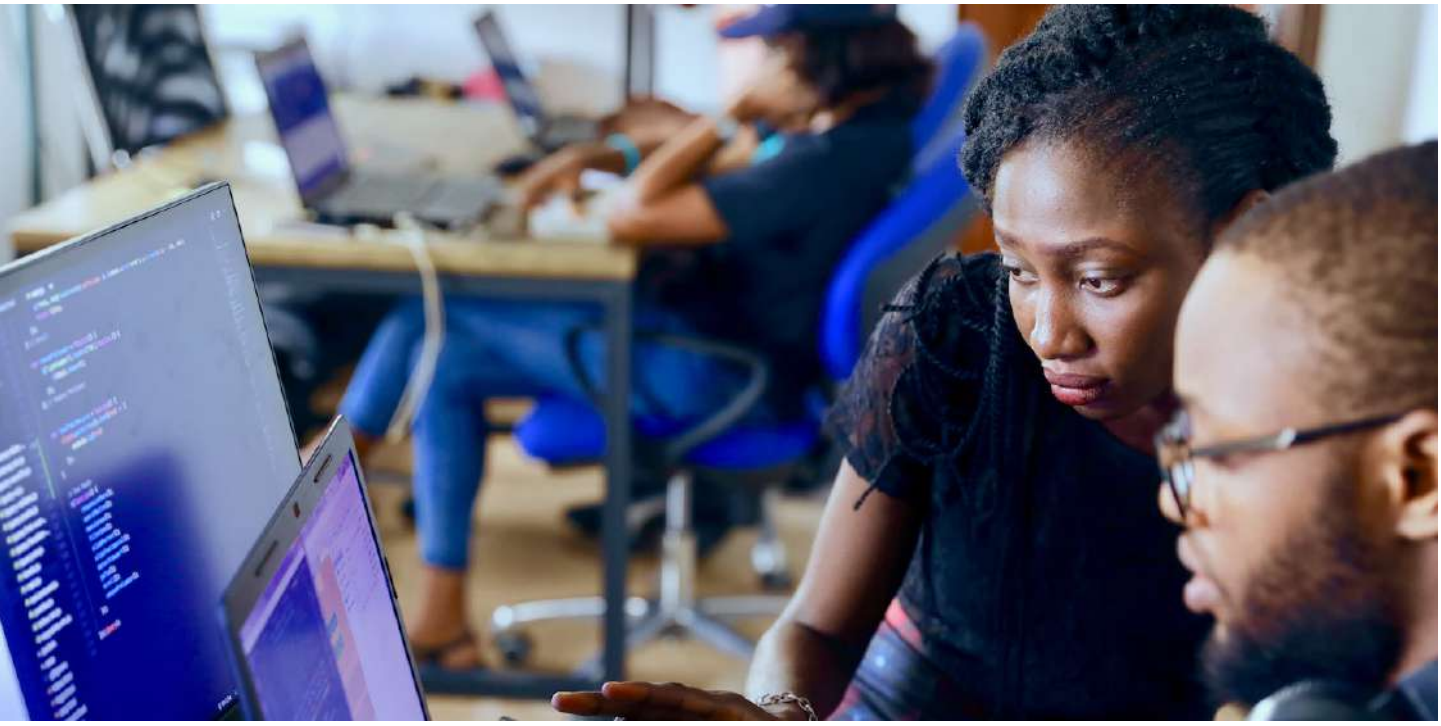
The Facebook Ad Library data between May 29th 2022 and 8th August 2022 included 3,827 ads from 3,319 pages in both English and Kiswahili. From the sum of the lower bound spend around 60% of the ad spends (at least KES 2.3 Million) were paid for using Kenyan shilling (KES) with the rest were paid for with foreign currencies including US Dollar (USD), Swiss Franc (CHF), Canadian Dollar (CAD) etc. Besides examining the overall descriptive statistics from the original dataset, we applied the upper tailed t-test on the demographic and geographic attributes.

57%

of political ads were targeted towards the 25-34 age group

The demographic attributes included age and gender. The results from the targeting summary show that a majority (57%) of political ads were targeted towards the 25-34 age group. This was despite the fact that the largest proportion of Facebook users in Kenya from May to August 2022 was between 18 to 24 years according to NapoleonCat.[65] Overall the ads targeted towards the youth (19-34) represented 83% of the total ads within the dataset. 10% of the sampled ads did not seem to have any specific age group target. Further analysis into the gender feature did not reveal any evidence of targeting by gender within our dataset with None having 100%.

Picture by disruptxn https://unsplash.com/photos/kwzWjTnDPLk



[65] https://napoleoncat.com/

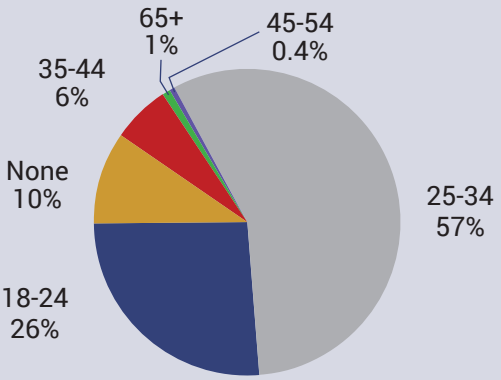


Figure 1: Distribution of Age group targeting by political ads

The examination of geographic variables (location) showed a general lack of geolocation target (at least using the former 7 provinces of Kenya). However, Nairobi showed signs of having some level of geo targeting. Despite this, the total number was significantly smaller compared to the total Nairobi Facebook users (4.6 million users) which accounts for 71% of Kenya`s Facebook users at the time.

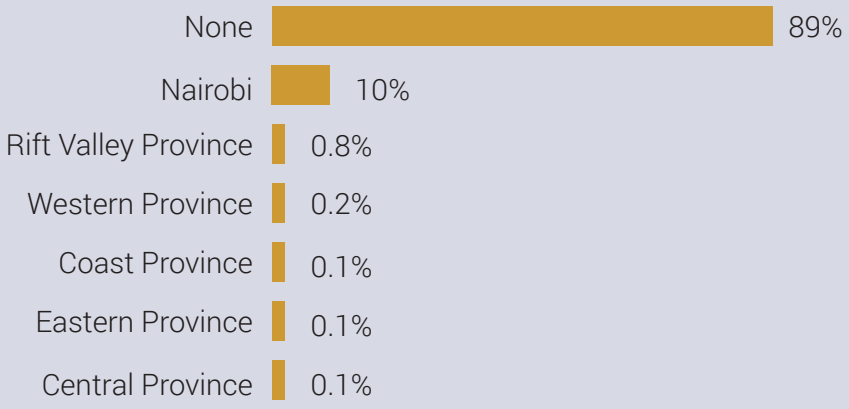


Figure 2: Regional targeting by political ads

Analysing Ad message

The three main topics arising from the LDA topic modelling analysis were: "Form ni bottoms up mtendakazi kenya inawezekana"(Topic 2), "Chagua maendeleo emergency clinics care"(Topic 1), "Support, People, Women & rights"(Topic 0). Topic 2 showed an inclination towards the voting for a political candidate while Topic 1 was inclined towards health care and wellbeing among the public. Topic 2 as identified by the LDA analysis had a more general theme around helping people, championing women as well as citizen's right. From these we may infer that both Topic 0 and Topic 1 were geared to a particular set of policies as opposed to Topic 2 which was geared towards support for a particular political candidate.

Dominant Topic	Proportion
Topic 0	51%
Topic 1	43%
Topic 2	6%

Table 1: Proportion of Dominant Topics within data

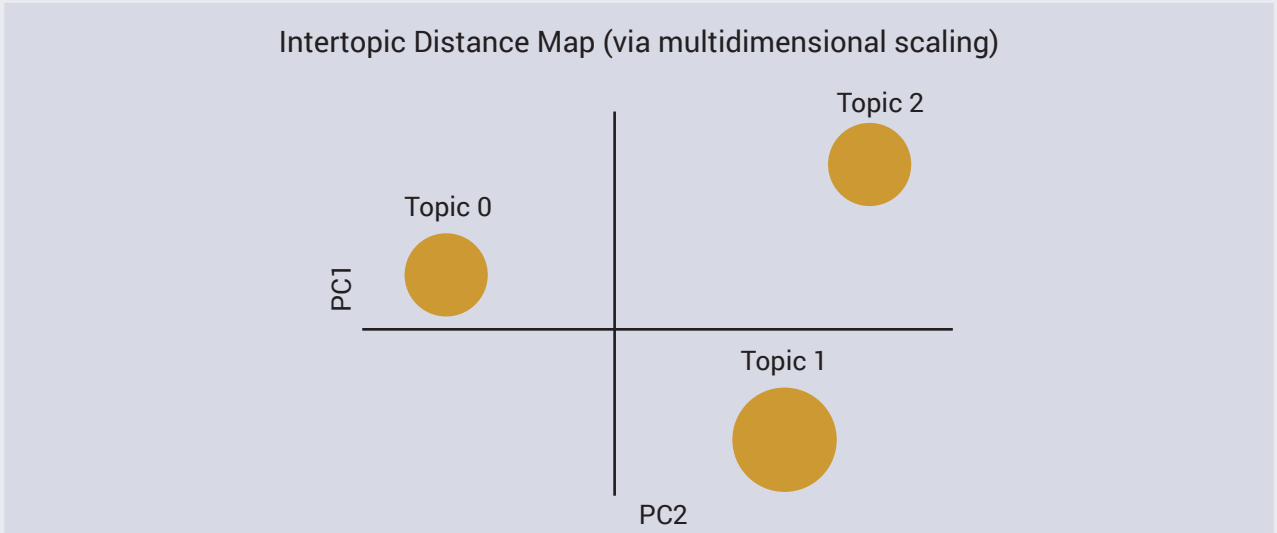


Figure 3: PCA representation of topics from LDA

Marginal topic distribution: 2% => 5% => 10%

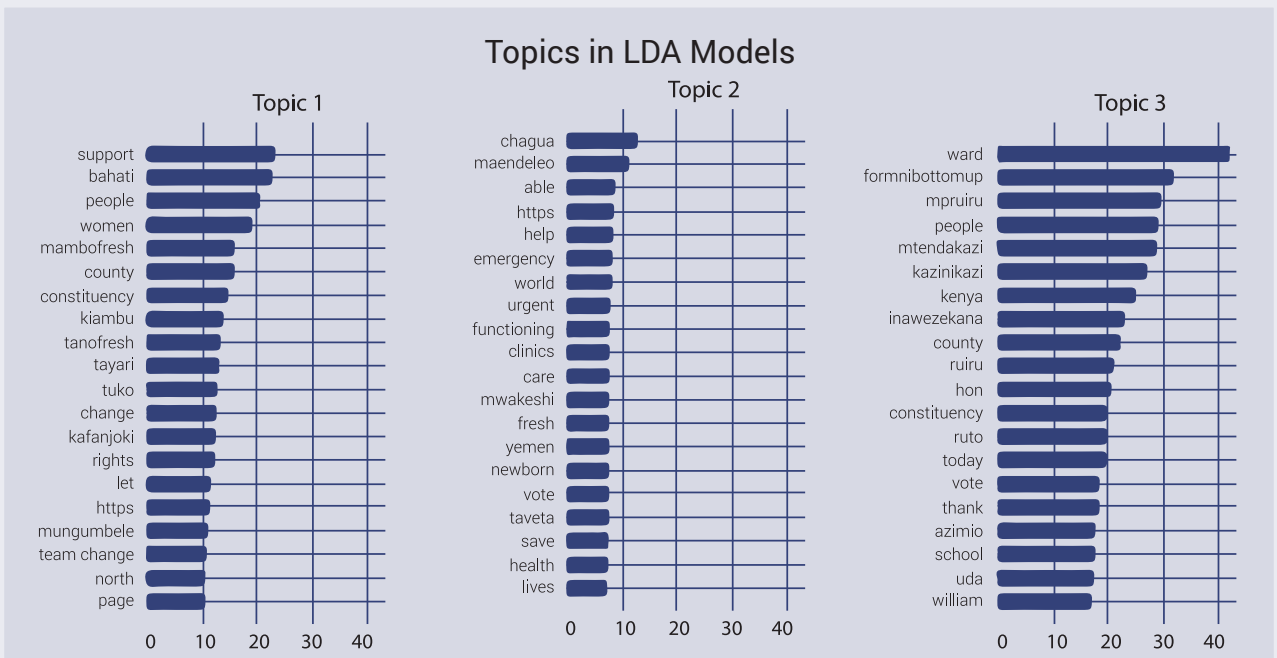


Figure 4: Distribution of key words across topics from LDA

Dominant Topic	18-24	25-34	35-44	45-54	65+	None
0	26%	57%	5%	0.5%	1.0%	10%
1	25%	57%	6%	0.3%	1.1%	10%
2	27%	60%	4%	0.6%	0.6%	8%
None	33%	46%	7%	-	0.8%	13%

Table 2: Age group distribution by Dominant Topics of political ads

Table 2 shows the relationship between the three main topics in the ads and the targeted age. The results show that the three topics all had a similar distribution in reach specifically gaining more traction with the youth (~84%) as opposed to other age groups.

Dominant Topic	Central Province	Coast Province	Eastern Province	Nairobi	None	Rift Valley Province	Western Province
0	0.1%	0.2%	0.1%	9%	89%	0.9%	0.3%
1	0.3%	0.3%	0.6%	8%	90%	0.9%	0.3%
2	-	-	-	13%	86%	1.2%	-
None	-	-	-	10%	89%	0.8%	-

Table 3: Regional targeting by Dominant Topic of political ads

From the table above we observe that, ignoring the ads without geotargeting settings, most Topics were aimed at Nairobi. Topic 2 was mostly geared towards Nairobi and Right Valley. A more granular breakdown of the 3 themes might revel instances of A/B testing across regions.

Regional Targeting

Target Region	18-24	25-34	35-44	45-54	65+	None
Central Province	40%	40%	-	20%	-	-
Coast Province	50%	33%	-	-	-	17%
Eastern Province	13%	50%	13%	-	-	25%
Nairobi	55%	38%	1%	-	-	7%
None	23%	59%	6%	0.4%	1.1%	10%
Rift Valley Province	58%	31%	-	-	-	12%
Western Province	56%	33%	-	-	-	11%

Table 4: Age group distribution by Target region for political ads

Table 4 shows the ad targeting based on regions and age groups in Kenya thus giving a picture of the ads that employed both regional targeting and age-group targeting. From the data above, it is clear that in most regions ads were targeted toward the youth vote in the country.

Topical, Demographic and Geographic Targeting

This section examines the political ads that were seen to have a specificity of message, narrowness of demographic characteristics (age and gender); and precision in regional targeting.

Target Region	Dominant Topic	18-24	25-34	35-44	45-54	65+	None
Central Province	0	50%	-	-	50%	-	-
	1	33%	67%	-	-	-	-
Coast Province	0	33%	33%	-	-	-	33%
	1	67%	33%	-	-	-	-
Eastern Province	0	-	-	-	-	-	100%
	1	14%	57%	14%	-	-	14%
Nairobi	0	56%	35%	1%	-	-	8%
	1	51%	44%	1%	-	-	3%
	2	55%	36%	-	-	-	9%
	None	67%	17%	-	-	-	17%
None	0	23%	60%	6%	0.4%	1.1%	10%
	1	23%	59%	6%	0.3%	1.2%	11%
	2	23%	63%	5%	0.7%	0.7%	8%
	None	28%	50%	8%	-	0.9%	13%
Rift Valley Province	0	62%	31%	-	-	-	8%
	1	60%	20%	-	-	-	20%
	2	-	100%	-	-	-	-
	None	100%	-	-	-	-	-
Western Province	0	80%	20%	-	-	-	-
		25%	50%	-	-	-	25%

Table 5: Ad targeting based on region, topic and age

Table 5 shows the distribution of micro-targeting across the different geographic, demographic and general topic themes. If we examine the two topics that showed elements of specific policy messages (Topic 0 and Topic 1) – 90%, specific geographic targeting 6% – 11%, and elements of age group targeting - 90%, only 8.7% of our sample dataset showed evidence of micro targeting, i.e., political advertising possessing a specific political theme, narrowness of demographic (age and gender) characteristics and the precision of geographic targeting.

If the definition of political-microtargeting is confined to messages that demonstrate a relative precision in terms of location, audience, and message, then we conclude that a relative minority of advertising – approximately 9% (at least on Facebook) met those criteria. According to the findings provided here, one or more of these factors are crucially absent from the majority of Facebook political advertising. Computational analysis finds that the resources for precise content-creation - which may be used to precisely target voters - was not leveraged by ad creators in Kenya's 2022 election cycle. It is one thing to properly segment a potential audience effectively; it is quite another thing to create issue-specific content that might be directed to such an audience. This limitation proves to be a problem even in the world of well-resourced candidates and political parties in developed countries.[66]

[66]Susan Delacourt, *Shopping for votes: How politicians choose us and we choose them* (Douglas & McIntyre Publishers 2013)

Further research could be done to uncover instances of A/B testing and come up with a more precise estimation of alternating messaging to provide deeper analysis of the general themes. This would aid in developing a more refined, and nuanced, understanding of the different levels of micro-targeting experienced in Kenyan elections. Not all micro-targeting carries the same precision and not all raise the same concerns about electoral manipulation and propaganda.

The findings also lead to the broader point that political micro-targeting, as a practice, not only needs more nuanced definition but also an understanding in the context of the entire network of campaigning organizations involved in the data-driven election. Understanding the "micro" in micro-targeting inevitably, therefore, requires an understanding of the "macro" conditions of political campaigning and of the larger operation of data-driven elections.

Picture by Crablinks Interactive https://unsplash.com/photos/NrQl0WJCtNM

F. LEGAL ANALYSIS

While the computational analysis detailed in the prior section determined the political micro – targeting was not prevalent in the 2022 Kenyan election, it still occurred and instances of it may increase in future electoral processes. It is important, therefore, to ascertain what legal protections are afforded to voters against the detrimental impacts of this practice. The sections below outline existing laws in Kenya that offer protections from the possible effects of political micro-targeting.

Existing laws applicable to microtargeting in Kenya

There is no specific legislation that addresses political microtargeting in Kenya. It is important to determine whether Kenya has the capability to curtail microtargeting practices in the absence of a single comprehensive law. The laws identified don't specifically mention the practice of microtargeting but the aspects that the laws deal with intertwine with the practice and therefore will be instrumental in regulation. After gathering and analysing existing data, the following laws were found to be applicable to political microtargeting namely:

i. The Constitution of Kenya

The Constitution of Kenya is the supreme law of the country and the right to privacy is enshrined in it. Every citizen is guaranteed the right to informational privacy as provided for in Article 31(c) of the Constitution. There have been various theories by different individuals on what informational privacy entails. Daniel Solove describes informational privacy as a right to have one's information 'treated thoughtfully to understand the disclosure of one's personal data and to participate meaningfully in the use of that data.' Political microtargeting undermines information privacy since it dwindles the voter's ability to have control over their personal information.[69]

The constitution of Kenya is the supreme law of the country and the right to privacy is enshrined in it.

The practice also threatens the political privacy of individuals by 'compromising the personal sphere' which is considered essential for democratic deliberation and self-determination. [70] Thomas Emerson views privacy as a zone in which the individual can 'think his own thoughts, have his own secrets, live his own life and reveal only what he wants outside the world.[71] Any breach on political data may stir certain ripple effects for instance voters may have 'diminished faith in publicly supervised political processes.[72] The provision on the right to privacy enshrined in the Constitution

[67] It provides that, 'Every person has the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed.'
[68] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet* < https://lawcat.berkeley.edu/record/1118208/files/fulltext.pdf > accessed 1 July 2022
[69] Rubinstein (n 6)
[70] ibid
[71] ibid
[72] ibid

plays a key role in protecting the political and information privacy of individuals. Political privacy is described as a 'public value that supports democratic political systems.'[73] Considering that the Constitution is the supreme law of the land, the provision on the right to privacy plays a significant role in regulating microtargeting since the respective authorities now have to come up with measures to ensure that the political and information privacy of voters is protected. To bring this into fruition, the Data Protection Act was enacted into law in 2019.[74] The legislation is discussed below in detail.

ii. The Data Protection Act 2019

The 2019 Data Protection Act regulates how personal data is processed and ensures that the data subject's data is processed[75] in accordance with the data protection principles provided for in the legislation.[76] Personal data should be processed with regard to the right to privacy of a data subject, [77] in a lawful, fair and transparent manner[78] and should be collected for specified and legitimate purposes.[79] The personal data should also be relevant to what is necessary in relation to the purposes for which it is processed.[80]

The data controller or data processor is in charge of handling the personal data of individuals and therefore should process it in accordance with the above principles. The Act defines a data controller as 'a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data.'[81] The data processor on the other hand means 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.'[82] When it comes to political microtargeting, there are two types of actors that could be regarded as data controllers namely 'the online platforms and the political actors.[83] The Bavarian Administrative Court in 2018 held that Facebook and the user of Audience should be considered joint data controllers.[84] The Court of Justice of the European Union (CJEU) have also supported this idea.[85]

One of the concerns of political advertising is the likelihood of violating the purpose limitation principle. The principle means that collection of personal data should be for specific and legitimate purposes. Section 25 (c) provides that data processors have the obligation to ensure that personal data collected is for specified and legitimate purposes. The processing of personal data for legitimate purposes is applicable in political microtargeting if the purpose would be to 'increase political or democratic engagement.[86] The collection of personal data for political microtargeting purposes goes against the legitimate purpose principle especially once it is collected by social media platforms and processed for political advertising based on 'an objective different from the original.[87] This provision is key in restricting microtargeting practices since it places confines on the processing of personal data.

The data minimization principle also plays an important role in regulating political microtargeting. Section 25

[73]ibid
[74]Data Protection Act 2019, the preamble provides that the purpose of the legislation is to 'give effect to Article 31(c) and (d) of the Constitution.'
[75]Data Protection Act 2019, section 3 (a)
[76]ibid section 3 (b)
[77]ibid section 25 (a)
[78]ibid section 25 (b)
[79]ibid section 25 (c)
[80]ibid section 25 (d)
[81]ibid section 2
[82]ibid
[83]Cristina Blasi Casagran and Mathias Vermeulen, *Reflections on the murky legal practices of political micro-targeting from a GDPR perspective* < https://academic.oup.com/idpl/article/11/4/348/6355314 > accessed 9 September 2022
[84]ibid
[85]ibid
[85]ibid
[87]ibid

(d) of the Act provides that the processing of personal data has to be 'adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed.' Applying this principle to microtargeting would mean that the personal data used to target voters are the 'minimum criteria that political actors need to fulfil their purpose.'[88] The principle would also require 'periodic reviews of the data held with deletion of the data items that are no longer necessary.'[89]

Consent is also required from a data subject before processing their personal data for a specified purpose.[90] The data belonging to a voter can therefore be collected for targeting and micro targeting purposes if they have given consent for it to be used for such purposes.[91] Since microtargeting involves direct marketing, the Act requires that where personal data is being used for commercial purposes, express consent must have been given by the data subject.[92] Additionally, due to the nature of such data, the rights and freedoms of a data subject may be at a high risk and therefore a data processor shall be required to perform a data protection impact assessment.[93]

Political microtargeting also involves profiling of voters so as to influence their voting behaviour. Profiling basically entails the evaluation of an individual's personal data to analyse or predict certain aspects about a person such as their habits, personality, political beliefs and many other aspects.[94] By analysing the personal data, targeted political messages can then be sent to a voter based even on their name since they identify someone's tribe and therefore likely to vote for a particular candidate. Since profiling involves the automated processing of personal data, the Data Protection Act provides that 'a data subject has the right not to be subject to a decision based solely on automated processing including profiling…'[95] Where a decision is made based on processing, the data processor is required to notify the data subject in writing.[96] These provisions will therefore be important in regulating political microtargeting since data processors are restricted from automated processing of personal data for profiling purposes without involving the data subject.

The legislation also provides for sensitive personal data and this kind of data includes a person's race, their biometric data and also their ethnic social origin.[97] The ethnic origin of a person can easily be identified by the name one holds and therefore this also becomes easy for political actors to target certain individuals.[98] In such a case, a name can be placed in the category of sensitive personal data. If a political actor desires to process such data they will have to satisfy the conditions for processing personal data[99] and one of the grounds for processing sensitive personal data provided for in Section 45 of the Act.

[88]ibid
[89]ibid
[90] ibid section 32 (1) provides that, 'A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.'
[91]Hashim Mude, 'Political Micro-targeting in Kenya: An analysis of the legality of Data-Driven Campaign Strategies under the Data Protection Act' (2021) 1(1) JIPIT 7-36
[92]Data Protection Act 2019, section 37 (1) (a)
[93]ibid section 31 (1) provides that, 'Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes,
a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.
[94]Privacy International, *Why we are concerned about profiling and microtargeting in elections* <https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections > accessed 7 October 2022
[95]Data Protection Act 2019, section 35 (1)
[96]ibid section 35 (3) (a)
[97]ibid section 2
[98]Mude (n 77) 19
[99]ibid

iii. The Data Protection (General) Regulations 2021

The regulations provide that certain measures should be taken by the data controller or processor when processing personal data on the basis of consent. A data subject will therefore be aware of the implications involved in processing personal data. Section 4 of the regulations lists the information that a data processor shall inform the data subject of and some of these include the right to withdraw consent, whether the personal data that will be processed shall be shared with third parties and also the kind of personal data collected.

Such measures will hinder political micro-targeting since they will ensure transparency is observed and political actors don't misuse personal data which they have obtained from data subjects. Additionally, a data processor who obtains consent from a data subject will be required to ensure that the consent was given voluntarily, it was specific to the purposes of processing and the data subject had capacity to give consent.[100]

The regulations also recognise that personal data can be used for commercial purposes through direct marketing and it occurs when a data controller or data processor advances commercial interests through 'displaying an advertisement on an online media site where a data subject is logged on using their personal data...'[101] The regulations provide that personal data can be used for direct marketing purposes by the data controller or data processor under certain conditions which include notification of the data subject that 'direct marketing is one of the purposes for which personal data is collected.[102] The other requirement is that the data subject should have 'consented to the use or disclosure of the personal data for the purpose of direct marketing.'[103] Direct marketing has the potential of being exploited for digital campaign purposes and the recipient of the targeted messages may not be aware that the messages are part of a political campaign.[104] Direct marketing is pivotal to the practice of political microtargeting since it involves sending of personalised communications to the data subject. Political campaigns are now using direct marketing to 'promote candidates and influence potential voters.[105] With the above conditions in place, the regulations will be essential in ensuring that personal data is handled in an appropriate manner before direct marketing takes place thus hindering the misuse of personal data for microtargeting purposes.

Political campaigns are now using direct marketing to promote candidates and influence potential votes.

The right to object to processing is recognised in the regulations and it is also applicable where processing is for 'direct marketing purposes which includes profiling...'[106] If a data subject objects to the processing of his or her personal data for instance where it is obtained for political micro-targeting purposes, he or she can request for erasure or destruction of the data.[107] The regulations also provide the procedures that will be followed whenever a data controller or processor receives such a complaint. The measures will therefore play a key role in restricting political micro-targeting practices.

[100]The Data Protection (General) Regulations 2021, section 4(3)
[101] ibid section 14 (2) (b)
[102]ibid section 15 (1) (b)
[103]ibid section 15 (1) (c)
[104]Privacy International, *Micro-targeting in Political Campaigns: A comparative analysis of legal frameworks* < https://privacyinternational.org/sites/default/files/2021-01/UoE_PI%20Micro-targeting%20in%20policital%20campaigns%20comparative%20analysis%202021.pdf > accessed 9 September 2022
[105] ibid
[106]The Data Protection (General) Regulations 2021,section 8 (4)
[107]ibid section 12

iv. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

The regulations 'provide for the procedure required for registration of data processors and controllers.'[108] The regulations will play a key role because without them the Data Commissioner would have a difficult time registering data processors and controllers and this includes political parties and candidates thus ensuring that the activities they engage in are monitored.[109] The regulations provide that a data controller or data processor is required to register as being a data controller or processor where personal data is processed for 'canvassing political support among the electorate.'[110] Political microtargeting involves many actors and these include: political advertisers, political parties, political consultants, online platforms, content service providers, data brokers and data analytics companies.[111]

Data brokers may act as controllers or processors 'depending on the degree of control they have over the processing.[112] Analytics companies can also be data controllers or data processors depending on whether they collect data on 'potential voters themselves or they process data originally collected by political parties.'[113] European national data authorities and also the Court of Justice of the European Union (CJEU) have supported the idea that social media companies which offer 'custom' audiences should be considered as joint controllers with the advertiser.[114]

Where political microtargeting doesn't involve online social media platforms, the political actors should be considered as sole data controllers.

Where political microtargeting doesn't involve online social media platforms, the political actors should be considered as sole data controllers.[115] The registration of all the political actors regarded as data controllers or processors will play an essential role in accountability of personal data use. If personal data is misused for political microtargeting purposes, the data processors can be traced and the appropriate action taken. The third schedule of the regulations requires political parties to register as data controllers and processors. This will assist in curtailing microtargeting by imposing a duty on data processors to handle personal data responsibly.

v. The Elections (Technology) Regulations, 2017

The regulations govern the use of electoral technology in elections and are enforced by the Independent Electoral and Boundaries Commission (IEBC). Part V of the regulations deal with information security and data storage. The commission is required to come up with mechanisms to ensure confidentiality of data and measures to protect against attacks on election technology.[116] These measures are important so as to protect voters' alphanumeric and fingerprint data from being misused for instance through political micro targeting.

[108]The Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021, section 3(1)
[109]Abdulmalik Sugow and Isaac Rutenberg, *Securing Kenya's Electoral Integrity: Regulating Personal Data Use* (1 October 2021) < https://www.theelephant.info/op-eds/2021/10/01/securing-kenyas-electoral-integrity-regulating-personal-data-use/ > accessed 20 July 2022
[110]Third schedule
[111]Casagran (n 69)
[112]ibid
[113]ibid
[114]ibid
[115]ibid
[116] The Elections (Technology) Regulations 2017 section 14

The IEBC maintains that its database has not been hacked to date since its data storage is not centralised. This is because it uses primary and secondary servers.[117] The Commission also confirmed that it has an external disaster data recovery site[118] which is in line with the requirements provided in section 25 of the Elections (Technology) Regulations.[119]The security of election technology is important so as to avoid any breach on the election website that may cause personal data to leak[120] thus being misused for political campaign purposes like political microtargeting. The regulations also require any person or telecommunication network service provider that becomes aware of any election technology vulnerability to notify the Commission.[121] Measures such as this guarantee adequate protection to data belonging to voters thus securing the data from misuse. An example of voter data breach is what happened in Mexico where names and addresses of 87 million voters could be accessed through Amazon's cloud computing site.[122]

vi. The Computer Misuse and Cybercrimes Act, 2018

One of the threats of political micro-targeting is that it has the capability of turning citizens into objects of manipulation and thus 'undermines the public sphere by thwarting public deliberation, aggravating political polarization and facilitating the spread of misinformation.'[123] The issue of misinformation is addressed in the Computer Misuse and Cybercrimes Act and it makes it an offence to misinform an individual with the intent that the data relied on shall be acted upon.[124] This provision will help curtail the practice of microtargeting since people will restrain from spreading false information targeted towards specified voters which if relied upon can misinform them.

Another threat of micro targeting is with regard to privacy and especially data breaches. Once a hacker realises that there is a loophole when it comes to protection of data belonging to individuals, they can access databases containing personal data[125] then misuse it. This offence amounts to unauthorised access and according to the legislation, it occurs when a person 'causes whether temporarily or permanently, a computer system to perform a function by infringing security measures with intent to gain access and knowing that such access is unauthorised…'[126] Prohibiting unauthorised access of a computer system will therefore play a fundamental role in curtailing misuse of voters' personal data that may be accessed and propagate microtargeting threats.

The Computer Misuse and Cybercrimes Act makes it an offence to intentionally or without authorisation intercept data and cause it to be transmitted to a computer system or telecommunication system.[127] This provision is important so as to protect personal data from cybercriminals who may access computer systems and intercept data and misuse it for microtargeting purposes or even for their own personal reasons that may be harmful to a voter's privacy. The provision also ensures that data processors who deal with the personal information of voters implement cybersecurity measures to protect the personal data of individuals.

---

[117]Dr. Robert Muthuri,Moses Karanja, Francis Monyango and Wanjiku Karanja, *Biometric Technology, Elections and Privacy In Kenya* < https://cipit.strathmore.edu/biometric-elections-privacy-kenya/ > accessed 20 July 2022
[118]ibid
[119]The Elections (Technology) Regulations 2017, section 25 (1) (a)
[120]IDEA, *Cybersecurity in Elections*< https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf > accessed 14 September 2022
[121]The Elections (Technology) Regulations 2017,Section 27(1)
[122]Colin J. Bennet, 'Voter databases, microtargeting and data protection law: can political parties campaign in Europe as they do in North America?(2016) 6 (4) International Data Privacy Law 261-275
[123] Frederick J. Zuiderveen, Judith Moller, Sanne Kruikemeier and Claes de Vreese, ' Online Political Microtargeting: Promises and threats for Democracy' (2018) 14 (1) Utretcht Law Review 82-96
[124]The Computer Misuse and Cybercrimes Act 2018, section 22(1)
[125]Zuiderveen (n 109)
[126]The Computer Misuse and Cybercrimes Act 2018, section 14(1)
[127]The Computer Misuse and Cybercrimes Act 2018, section 17(1)

Picture by Sora Shimazaki https://www.pexels.com/photo/a-person-dropping-his-vote-in-white-box-5926254/

vii. Guidance Notes for Electoral Purposes

In 2022, the Office of the Data Protection Commissioner published a guidance note meant to assist data controllers and data processors who deal with voters' personal data, including sensitive personal data, members of political parties' personal data to understand their obligations under the Data Protection Act, 2019. The Guidance Note states that it applies solely to the processing of personal data on voters (or potential voters) and the processing of personal data for the purposes of creation and maintenance of member registers. On microtargeting, the Guidelines on the right not to be subject to automated decision making states that voters have the right not to be subject to decision significantly affecting them based solely on an automated processing of data without having their views taken into consideration or without human intervention. Still on automated decision making, the Guidelines also state that when voters receive or are subjected to automated delivery of digital political advertising, they have the right to know why they are receiving such advertising material or receiving the "ads". [128]

To conclude this section, the existing laws and regulations discussed above play a significant role in governing how data regarding voters should be handled which is important in protecting data subjects. However, there are certain gaps in these legislations that need to be addressed such as the lack of precise rules on the use of personal data for political micro-targeting and also lack of a clear definition of what political advertising entails. A single comprehensive law dealing with political microtargeting may be required since this is an emerging area and developments in the ICT sector will require legislators to come up with laws addressing specific sectors being affected by technological advancement including the political arena.

[128] Office of the Data Protection Commissioner, Guidance Notes for Electoral Purposes

G. POLICY RECOMMENDATIONS

The various provisions in the legislations discussed in the previous sections are important when it comes to regulating political microtargeting. However, microtargeting involves other components that are beyond the scope of the provisions enshrined in the above laws. The first shortcoming of the above legislations is that they deal with personal data generally for instance the Data Protection Act or according to the purposes of the specified legislation for instance the elections (technology) regulations which deal with election matters. Political micro targeting is a separate practice on its own which requires detailed provisions on the use of personal data for specifically that purpose. The provisions ought to describe in detail how personal data will be handled for microtargeting purposes thus making it easy for respective authorities or data subjects to take appropriate action in case an issue arises. The gap in the identified laws is that they lack provisions addressing microtargeting as a separate subject or matter.

A number of countries have come up with initiatives to regulate online political micro targeting and Kenya can learn from some of these countries. These countries include Canada, France, Ireland, Singapore and the United States. In Canada, the Elections Modernization Act amended the Canada Elections Act and came up with new transparency rules for elections. It also regulates campaign advertising through social media platforms such as Facebook, Google and Twitter.[129]

The Elections Modernization Act introduced the term "online platforms" and it includes, 'an internet site or internet application whose owner or operator in the course of their commercial activities, sells, directly or indirectly, advertising space on the site or application to persons or groups.'[130] The introduction of this term was important because it extended the regulatory extent of the Canada Elections Act. The definition also applies to online platforms whereby election advertising also takes place.[131] The Canadian legislation gives an elaborate definition of what an online platform is and what it entails. The rapid internet growth in Kenya has also shifted the way advertising takes place from traditional means of advertising to now using online platforms for advertisements. Including a similar provision that defines and describes what online platforms entail in the election laws will provide a clear guideline on what exactly they are and also extend the scope of election regulation in Kenya.

The Act also requires that 'the owner or operator of an online platform that sells, directly or indirectly, advertising space to the following persons and groups shall publish on the platform a registry of the persons' and groups' partisan advertising messages and election advertising messages published on the platform during that period:

i. A registered or eligible party

ii. A registered association

iii. A nomination contestant

[129] Anna Reepschlager and Elizabeth Dubois, *New election laws are no match for the internet*< https://policyoptions.irpp.org/fr/magazines/january-2019/new-election-laws-no-match-internet/ > accessed 27 June 2022
[130] Elections Modernization Act 2018, section 206(2) amending section 319 of the Elections Act.
[131] Michael Pal, *Evaluating Bill C-76: the Elections Modernization Act* < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572737 > accessed 27 June 2022

iv. A potential candidate or a candidate; or

A third party that is required to register under subsection 349.6 (1) or 353(1).' [132]

The owner or operator of the online platform is required to keep the information in the registry for five years thus preventing the information from being destroyed when it is required urgently such as in cases of litigation or when there are 'investigation for breaches of the Elections Act.'[133]

The record keeping requirement is fundamental because it enhances transparency. It may also include a copy of the qualified political advertisement, a description of the audience targeted by such advertisement and even the average rate charged for the advertisement.[134] In order to increase accountability, the record keeping requirement can be included in the Kenyan election laws so as to simplify the public inspection process and also to identify the people behind the political advertisements. This enables the appropriate action to be taken in case of a breach of the respective electoral law.

In France, Article L 163-1 provides that, 'during the 3 months before the first day of the month of general elections until the date of the ballot, online platforms must display to users information on:

i. the identity of the individual or on the company name, registered office and corporate purpose of the legal person and of the person on whose behalf, where applicable, it has declared that it is acting, which pays for the promotion of content related to a debate of general interest;

ii. use of personal data when promoting content related to a debate of general interest;

iii. the amount received in return for the promotion of such content when the amount exceeds a determined threshold, which should be made public.[135]

The above provision is an example of the disclosure requirement that is fundamental in online political advertisements regulations. Disclosure requirements are important because they enable interested parties like the public and also the media to inspect records that may be hidden from them.[136] The requirement is also important because it provides details of the organisation or individual's name that requested 'to place or paid for the advertisement.'[137] This enhances transparency of online political ads and also ensures that personal data is not misused. Having a similar provision in the Kenya electoral laws will enable voters to be aware of the individuals behind the advertisement and it will also complement the Data Protection Act 2019 as the provision will focus specifically on personal data use in online political advertisements.

The same Article L 163-1 also has a record keeping requirement which requires that online platforms create a register of promoted content.[138] Article L.52-1 of the France Electoral Code also prohibits that during the six months before an election, 'the use, for the purpose of election propaganda, of any commercial advertising in the press or any means of audio visual communication.'[139] The prohibition of commercial advertising is key in ensuring that voters are not swayed towards a particular political figure or party. Additionally, in 2018 France introduced other rules under Article L.163-1 providing that three months prior to elections, online platforms should provide users with information about who paid for the 'promotion of content related to a debate of

[132]Elections Modernization Act 2018, section 325.1(1)
[133]Pal (n 117)
[134]Carolina Menezes Cwajg, *Transparency Rules in Online Political Advertising: Mapping Global Law and Policy* (October 2020) <https://www.ivir.nl/publicaties/download/TransparencyRulesOnlinePoliticalAds2020.pdf > accessed 27 June 2022
[135]ibid
[136]Cleveland Ferguson III, *Disclosure Requirements* < https://mtsu.edu/first-amendment/article/946/disclosure-requirements > accessed 27 June 2022
[137]Cwajg (n 120)
[138]ibid
[139]Tom Dobber, Ronan O Fathaigh and Fredrik J. Borgesius, 'The regulation of online political micro-targeting in Europe' (2019) 8(4) Internet Policy Review 1-20

general interest.'[140] With the rapid increase of social media in Kenya, information spreads really fast. Politicians have also been accused of spreading election propaganda during the election period. By including a provision that limits online political advertising before elections in Kenya, influence on voters to vote in a specific way will be reduced and they will not be easily swayed towards voting for a particular candidate or political party

A provision limiting the period when online political advertising is allowed will also help to avoid some of the potential risks associated with microtargeting such as manipulating what voters see and read by use of sophisticated algorithms thus clouding their freedom of choice.[141] As an alternative, moderation of advertisements can be done during that period but if the information influences the voters to a large extent then measures prohibiting the dissemination of such advertisements can be implemented.

In Singapore, they have a Code of Practice for Transparency of Online Political Advertisements which is also known as the Political Advertisements Code. The Code 'sets out the obligations that prescribed digital advertising intermediaries and internet intermediaries have to comply with to enhance transparency of online political advertisements.'[142] It defines what political advertisement entails.[143] The definition of political advertisement is also found in other regulations dealing with online political advertisements. A clear definition of political advertisement should include what it entails for instance whether it includes search engine marketing or video advertisements and also the kind of political message it communicates. Just like the Political Advertisements Code in Singapore and many other jurisdictions, it is fundamental that online political advertisement and what it entails is enshrined in the Kenyan electoral laws since it will help to avoid ambiguity.

The Code also has a disclosure requirement for online political advertisements.[144] Additionally, there is a record keeping requirement provided by the legislation and it provides that 'a record of all such online political advertisements, regardless of whether the advertisement has been removed by the person or organisation who requested or paid to place the advertisement', must be kept and made available for viewing by the POFMA office…'[145] Just like in France and Canada, the disclosure and record keeping provision plays a fundamental role in enhancing transparency of online political advertisements. This indicates that the requirements are crucial in electoral laws and therefore when coming up with a regulation on political microtargeting in Kenya these requirements are among the key ones that should be considered when coming up with a robust legislation.

In the United States of America (USA), some states have come up with laws to regulate online political advertising. For instance in Maryland, there exists the Online Electioneering and Transparency and Accountability Act and it defines an online platform as, 'any public-facing website, web application or digital platform including a social network, ad network or search engine..'[146] Also under the Act, an online platform shall be made available for public inspection.[147] The Act defines electioneering communication and it includes '….a qualifying paid digital communication or an advertisement in a print publication that refers to a clearly identified candidate or ballot issue...'[148]

[140]ibid
[141]IDEA (n 1)
[142]Paragraph 4
[143]Paragraph 3(a) of the Code provides that, 'political advertisement means an advertisement or paid content that can reasonably be regarded as being directed towards a political end.'
[144]Paragraph 6 (b) provides that, 'Disclosure notices must display the name(s) of the person(s) or organisation(s) that requested to place or paid for the advertisement and also Disclosure notices shall be accessible.
[145]Paragraph 6(c)
[146]Cwajg (n 120)
[147]ibid
[148]ibid

The inclusion of a social network in the definition of an online platform is important because there has been a rapid increase in the use of the social network sites in Kenya. It is also easy to target voters using social network sites since many people share information on these platforms. It is reported that as of January 2021, the total number of social media users in Kenya was 11 million.[149] Therefore incorporating social network or social media in the definition of an online platform will be applicable in Kenya's context and this will therefore broaden the scope of the definition provided in the applicable legislation.

Other initiatives in the United States include: the New Jersey Legislature amendment, the Bolstering Online Transparency Act and Social Media Disclose Act which are both from California, the New York Election Law Rules and Regulations amendments, Vermont General Assembly amendment, Washington State Legislature amendments and Wyoming State Legislature amendment.

In Netherlands, the Dutch Code of Conduct Transparency Online Political Advertisements was published so as to address election transparency issues and disinformation in the digital sphere.[150] It also covers paid online political advertising.[151] In part 3.2 of the code, political parties commit to 'refrain from psychological profiling for targeting purposes in online political advertising.'[152] Also online platforms commit to 'develop and enforce relevant transparency mechanisms' with regard to political advertising.[153] The Netherlands legislation introduces a new dimension in online political advertisements and this involves the aspect of psychological profiling for targeting purposes. Political parties are regarded as data controllers or processors and therefore they have the responsibility of ensuring personal data is handled well. The provision could be applied in the Kenyan context and also included in the Kenyan electoral laws to avoid a repetition of microtargeting incidences experienced in Kenya and other countries like the United States.

11million
the number of Facebook users in Kenya in 2021

The proposed European Union regulation on the transparency and targeting of political advertising is another legislation which aims to 'protect natural persons with regard to the processing of personal data by laying down rules on the use of targeting and amplification techniques in the context of political advertising.'[154] The proposed regulation defines what political advertising entails.[155] Another key requirement that the legislation considers essential is transparency for political advertising services. The proposed regulation provides that 'political advertising services shall be provided in a transparent manner.'[156] The regulation also lays down certain requirements that must be met by controllers when they use targeting or amplification techniques. One key requirement is that the controllers shall 'provide together with the political advertisement, additional information necessary to allow the individual concerned to understand the logic involved and the main parameters of the technique use…'[157]

[149] Simon Kemp, *Digital in Kenya: All the Statistics You Need in 2021* < https://datareportal.com/reports/digital-2021-kenya#:~:text=Social%20media%20statistics%20for%20Kenya,total%20population%20in%20January%202021. > accessed 19 September 2022

[150] CounteringDISINFO, Dutch Code of Conduct Transparency Online Political Advertisements < https://www.counteringdisinformation.org/interventions/dutch-code-conduct-transparency-online-political-advertisements >accessed 27 June 2022

[151] IDEA, *Dutch Code of Conduct Transparency Online Political Advertisements*< <https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf > accessed 27 June 2022

[152] ibid

[153] ibid

[154] Proposal for a Regulation of the European Parliament and the Council on the transparency and targeting of political advertising

[155] Article 2(2) (a) and (b) provides that 'political advertising means the preparation, placement, promotion, publication or dissemination by any means of a message by, for or on behalf of a political actor unless it is of purely private or a purely commercial nature or which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour.

[156] Article 4

[157] Article 3 (c)

Online political advertising regulations should include transparency of political advertisements[158] as an important feature of online political advertising. This is because it provides clarity on advertisers, protocols and spending.[159] Therefore through transparency, people are able to know 'who is behind an ad and how much money parties and candidates invested in online advertising.'[160] It is important to have a provision on transparency when formulating a Kenyan law on microtargeting because people should know 'who is targeting them and why they are being targeted.'[161] Also, through transparency in data use, individuals can gain a greater understanding of the impact of online political advertising, especially researchers.[162]

Definition of political advertisement and disclosure of information relating to political advertising yet again features in this proposed regulation. In the Kenyan context, the mentioned provisions can be factored in when creating a legislation that deals with political microtargeting. As illustrated above in the other legislations, disclosure requirements and political advertisement definition are key in online political advertising legislations and therefore when enshrining these provisions, legislators in Kenya can assess the provisions from different legislations then formulate similar provisions that are applicable in the Kenyan context.

[158] The General Data Protection Regulation (GDPR) defines the principle of transparency in Recital 58 and it requires that 'any information addressed to the public or to the data subject be concise, easily accessible and easy to understand and that clear and plain language and additionally where appropriate, visualization be used.'
[159] International Institute for Democracy and Electoral Assistance, *Online Political Advertising and Microtargeting: The Latest Legal, Ethical, Political and Technological Evolutions* (18 June 2020)< https://www.idea.int/sites/default/files/publications/online-political-advertising-and-microtargeting-the-latest-legal-ethical-political-and-technological-evolutions-en.pdf > accessed 20 July 2022
[160] ibid
[161] ibid
[162] ibid

H. CONCLUSION

Political microtargeting is an emerging phenomenon and from the illustrations described in this study from other countries and also in Kenya, it is important for legislators to come up with robust laws addressing it. This is because it has its own threats which if not addressed can have a negative impact on voters. The laws applicable in Kenya can only regulate the practice to a limited extent and not holistically.

The external regulatory initiatives discussed in this study seem to follow a similar pattern when it comes to regulating political microtargeting. Some common aspects in the legislations include: the definition of an online platform as illustrated in the Elections Modernization Act from Canada and the Online Electioneering and Transparency and Accountability Act from Maryland, definition of political advertising as illustrated in the proposed European Union regulation on the transparency and targeting of political advertising and the Singapore Political Advertisements Code, obligations that digital advertisers must meet, record keeping and transparency requirements as can be seen in the Elections Modernization Act from Canada and the Singapore Political Advertisements Code. These are just some of the crucial provisions that can inform legislators in Kenya on what to include when formulating a robust law on political microtargeting.

Considering the rapid digitisation in Kenya, it is possible for Kenya to incorporate most of the provisions discussed in this study. The reason for this is because digitisation is now a key component in many sectors in Kenya. In the same way that there are election technology regulations, it is possible for legislators to formulate regulations specifically addressing online political microtargeting and advertisements.

ANNEX 1

HOW MICROTARGETING TAKES PLACE

1

Data Subject

By using various platforms the data subject shares information involving various aspects

2

Data Controller

The data which involves large data sets is then collected by the data controller and analysed

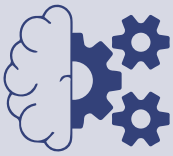
3

Analysis of the data collected

The data collected is studied and analysed by use of predictive modelling that matches an individual's personal characteristics with their political beliefs

4

Processing of images



Once the analysis has been done messages that align with the data subject's interests are processed and disseminated

5

Microtargeting

The disseminated messages are then targeted towards the data subject whose data has been analysed

6

Influence

The data subject receives messages or advertisements aligning with his or her interests eventually influencing the individual to identify with the message conveyed

This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.


ADULT
SCHOOL
BEGINNERS