Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 3, Issue 1 (2023) p.123-167
https:doi.org/10.52907/jipit.v3i1.259

Beyond the Ballot: A Comparative Analysis of Political Microtargeting Practices and Regulations in Kenya and Nigeria

*Joshua Kitili**

ABSTRACT

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 larger scale and with high levels of specificity. For political parties, better clarity leads to hyper-individualized communication in a process known as microtargeting. Critics argue that political microtargeting can directly manipulate and suppress voters, exacerbate polarization, perpetuate misinformation, and indirectly lead to long-term effects by encouraging political parties to ignore individuals whom they deem unlikely to vote or those who are digitally excluded. This paper studies political microtargeting in Kenya and Nigeria because of data-driven campaigns that have been observed in these jurisdictions in the past and due to the increased reliance on social media platforms that political actors are utilizing to influence voters. It argues that political microtargeting is an issue of concern and therefore, using Kenya and Nigeria, it pushes the agenda that countries in the Global South should implement policies and regulations to curtail the negative impact of the practice. To examine the extent of political microtargeting in both Kenya and Nigeria, this paper employs a multi-phase approach that involves an analysis of paid Facebook advertisements in both countries during the past election periods.

Keywords: Political Microtargeting, Algorithmic Politics, Social Media Platforms, Data-Driven Campaigns, Election

* Advocate of the High Court and Research Assistant at CIPIT. Master of Laws degree in Information Technology and Telecommunications Law from University of Strathclyde. Email: jkitili@strathmore.edu

TABLE OF CONTENTS

I. INTRODUCTION

The practice of political Microtargeting, 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 (Papakyriakopoulos *et al*., 2018). Microtargeting is a multi-step process that commences with the collection of data to analyze it with the aim of understanding people's behavior and opinions (Borgesius et al., 2018). The collection of data is followed by a categorization of individuals based on their inclinations such as similar concerns and opinions over issues (Borgesius *et al*., 2018).

Political microtargeting often involves the analysis of large data sets and the use of predictive modeling that matches an individual's personal preferences with their political beliefs so as to produce a desired voting decision from that individual (Rubinstein, 2014). Targeted personalized messages by political actors are later disseminated to the relevant audience (Borgesius *et al*., 2018).

Political microtargeting has attracted its fair share of criticism due to its recorded harmful effects on individual privacy and the democratic values of a country (The Guardian, 2018). For example, the ruling party in India uses in-depth demographic profiles to target voters based on caste or religious demographics (Daxecker & Milan, 2021). The microtargeting practice in India is often reliant on misinformation and hateful rhetoric and has a harmful effect on the democratic public discourse (Daxecker & Milan, 2021). 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 (Philippi, 2017).

While the true impact of microtargeting is yet to be seen in many countries other than a few that have been documented in the recent past, its effects should not be understated (Bodo *et al*., 2017). 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 the voter population (Pocyte, 2018). Individual privacy threats include the misuse of voters' data (Borgesius *et al*., 2018).

Whereas there are overlapping similarities between microtargeting and disinformation, this paper primarily focuses on microtargeting. Disinformation is mainly concerned with the intentional dissemination of misleading and wrongful information which seeks to 'shape perceptions around some aspect of political discourse' whereas microtargeting involves the use of predictive modeling to produce a desired voting decision (Disinformation: The Legislative Dilemma, 2020).

The most notable example of political microtargeting in Africa is the Cambridge Analytica scandal. The British data analytics firm allegedly deployed psychological profiling based on social media data to predict and influence voter decisions (Cadwalladr, 2018). The exposé famously known as 'the Cambridge Analytica-Facebook scandal' revealed that the firm had obtained data from an approximated eighty-seven million Facebook users via a third-party app and created psychographic profiles on them for political microtargeting (Kang & Frenkel, 2018). Specifically, in 2013, a 'Big-Five' personality test was circulated by Analytica via an app that had participants agreeing to share their Facebook data through the app for academic use (Hu, 2020). These included their identities, addresses, friend networks, and 'likes' (Granville, 2018). Though Facebook permitted app developers to collect data from users' friends, it prohibited sharing this data with third parties (Kroll, 2018).

Realizing the extensive use of social media in the African continent, this paper discusses political microtargeting using Kenya and Nigeria as case studies in light of their recent elections. The paper is divided into six parts. Part I is the introduction. Part II provides an overview of microtargeting in Kenya and Nigeria focusing on the threats that emanate and that might affect citizens as a result of microtargeting practices. Part III

delves into the data collection methodology employed and the overall results of the computational analysis in both regions. Part IV discusses the laws that are applicable to the practice of political microtargeting in both countries. This section also analyzes the laws in detail in lieu of a comprehensive microtargeting law that is lacking in both jurisdictions. Part V discusses policy recommendations derived by employing a comparative approach with other jurisdictions and Part VI concludes the paper.

II. THE STATE OF POLITICAL MICROTARGETING IN KENYA AND NIGERIA

In Kenya, a former executive of 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 (BBC, 2018). The data analytics firm stated that the surveys conducted covered 'key national and local political issues, levels of trust in key politicians, voting behaviors/intentions, and preferred information channels' (BBC, 2018). As a result, the company described its operations for the 2013 Kenyan elections as 'the largest political research project ever conducted in East Africa' and further admitted to using tribal divisions in its political messaging (Crabtree, 2018).

The firm is suspected to have used the large-scale data gathered from Kenya's publicly available voter registration databases and the data it collected from Facebook to conduct online political Microtargeting on digital platforms to sway voters' decisions (Sugow & Rutenberg, 2021). 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' (Meta, n.d.). Custom audiences allow advertisers to create audience segments that they want to include or exclude in paid political advertise-

ments (Lambe & Ricks, 2020). 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' (Lambe & Ricks, 2020). Look-alike audiences allow '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' (Lambe & Ricks, 2020). Presumably, tools like this are built on the psychographic profiles that the firm built from the data it collected.

In Nigeria, social media has become a very potent weapon of politics (PeterSide, 2022). Statistically, there were thirty-three million social media users in Nigeria as of January 2021 (DataReportal., 2021). The 2015 elections saw the beginning of a spike in online political campaigning, particularly on Twitter (now known as X) and Facebook. For the 2023 general elections, there were already signs that the amount of digital political advertising would rise even more. It is safe to assume that a substantial number of voters have access to social media, meaning that social and online media have almost replaced the combined mix of other media as critical avenues of communication in social and political matters (Peterside, 2022).

A. Implications and risks of microtargeting

1. Invasion of privacy and data breach

One of the implications of microtargeting is the 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, by tracking people's use of the internet, a company can generate a 'database of individuals and their interests' (Borgesius *et al.*, 2018). An example of an invasion of privacy is what happened in 2011 in Ireland when there was interference on Fine Gael's website by denial-of-service attacks that resulted in personal details of up to two thousand users of the site being compromised (Bennett, 2016).

Data is prone to cybercrime offenses especially if adequate measures are not taken to implement protection mechanisms. Offenses where a device is the target can interfere with data used and stored in the device. These offenses often target the gaining of unauthorized access to a device or computer system, causing unauthorized damage to computer data and unauthorized interception of computer data (Clough, 2010).

Where personal data has been collected for microtargeting purposes and adequate measures have not been put in place to protect the data, hackers or unauthorized persons can access the databases containing the personal data and misuse it. For example, in 2017, the U.S. Republican Party contracted a marketing company that suffered a data breach thus exposing the personal data belonging to almost two hundred million US citizens (Borgesius *et al*., 2018).

Additionally, the personal data collected for microtargeting purposes can be used for other purposes which can 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 (Accessnow, 2018). 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' (Accessnow, 2018).

2. Manipulation of voters

Voter manipulation can be exercised using, 'tailored information that maximizes or minimizes voter engagement' (Borgesius *et al*., 2018). The targeted information can be false and still have maximum impact. William Gorton (2016) warns that microtargeting facilitates the spread of misinformation (Borgesius *et al*., 2018). Cambridge Analytica is a good example because it has often been accused of overselling its capabilities in the elections in which it participated (Chen & Potenza, 2018).

In particular, Analytica's claim that it could sway voters' decisions by sending targeted messages attuned to their psychological profiles has been scrutinized (Chen & Potenza, 2018). The nexus between psychological profiling and political Microtargeting on voter decision-making is thought to be inadequately proven by existing research (Chen & Potenza, 2018). This is not to say that targeted advertising based on psychological characteristics is generally ineffective. In a relatively recent study, Matz *et al.*(2017) demonstrated that designing Facebook advertisements based on psychological factors 'resulted in up to forty percent more clicks and up to fifty percent more purchases than their mismatching or impersonalized counterparts' (Matz *et al.*, 2017, p.12714). Moreover, it has been argued that influencing political behavior through psychographic profiling and microtargeting might be drastically different from the consumer decision-making context studied by Matz *et al.* (Chen & Potenza, 2018).

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

3. 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' or the political party has high expectations of winning elsewhere (Borgesius *et al.*, 2018). Additionally, certain voters deemed not likely to vote can be excluded from receiving political messaging, essentially distancing them from meaningful political discussion (Gorton, 2016).

III. DATA COLLECTION METHODOLOGY AND COMPUTATIONAL ANALYSIS

In an effort to gain a clearer understanding of the role of microtargeting in both the Kenyan and Nigerian elections, this paper conducts an analysis of the political advertisements on Facebook during the official campaign period in the 2022 Kenyan elections and 2023 Nigerian elections. The author chooses to focus on Facebook as the platform of study due to the high percentage of individuals who utilize the platform. As of March 2022, twelve million Kenyans used Facebook. Facebook's ad reach in Kenya was equivalent to seventeen-point nine percent of the total population (Kemp, 2022). In Nigeria, thirty-eight million Nigerians were already using Facebook as of February 2023 and this accounted for seventeen percent of the entire population (Napoleon Cat, 2023).

A. Facebook data collection

In 2019, Facebook had to introduce its Ad Library–a feature that allows users to track a repository of adverts that have been placed on the platform, using location, topic, and timeline as filters (Howes, 2023). The platform, which was primarily introduced due to concerns about transparency in political advertising, includes three features: the Meta Ad Library, the Ad Library Report, and the Meta Ad Library API–a more sophisticated feature requiring a basic knowledge of coding to conduct customized searches of ads on Facebook (Alayande, 2022).

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.): start and end date when the ad ran, the ad copy, the 'ad creative', which one 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 (Crowdtangle, n.d.).

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' (Facebook, n.d.). Thus, when an ad appears on the 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.

Rather than creating a developer account, or installing a browser plug-in, the author relies on the public version of the ad archive for this study. 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 advertisement, what province(s) the ad was displayed in, and the age range and gender of the people who saw this ad.

Data collection in Kenya began on 29 May 2022 (the official campaign kick-off date) and ended one day before the General election, 8 August 2022 (IEBC, 2022). The data was collected by accessing Facebook's ad archive. In total, the results indicated that the dataset comprised three thousand three hundred and

nineteen Facebook ads. In Nigeria, the data was collected from 28 September 2022 (The Nation, 2022) until 24 February 2023 (one day before the General election) (IFES, 2023), which resulted in a dataset of nine thousand sixty-one Facebook ads.

B. Computational analysis and regional findings

1. Kenya

Microtargeting occurred at different levels and varied according to identified locations, demographics, and topical themes. A majority (fifty-seven percent) of political ads were targeted towards the twenty-five to thirty-four years old age group. This was despite the fact that the largest proportion of Facebook users in Kenya from May to August 2022 was between eighteen and twenty-four years according to NapoleonCat (2022). Overall, the Facebook Ad Library data indicated that ads targeted towards the youth (nineteen to thirty-four years old) represented eighty-three percent of the total ads within the dataset while ten percent of the sampled ads did not seem to have any specific age group target. Further analysis of the gender feature did not reveal any evidence of targeting by gender within the dataset.

From the Facebook data collected, the examination of geographic variables (location) showed a general lack of geolocation targets (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 (four million six hundred thousand million users) which accounts for seventy-one percent of Kenya`s Facebook users at the time.

The topics analyzed are: 'Form ni bottoms up mtenda kazi Kenya inawezekana' (Topic 2); 'Chagua maendeleo emergency clinics care' (Topic 1); and 'Support, people, women & rights' (Topic 0). Topic 2 showed an inclination towards voting for a political candidate while Topic 1 was inclined towards health care and wellbeing among the public. Topic 2 had a more general theme around helping people and championing women as well

as citizen's rights. It can also be inferred 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. All three topics also had a similar distribution in reach, specifically gaining more traction with the youth eighty-four percent) as opposed to other age groups. In terms of regional targeting, most topics were aimed at Nairobi.

2. Nigeria

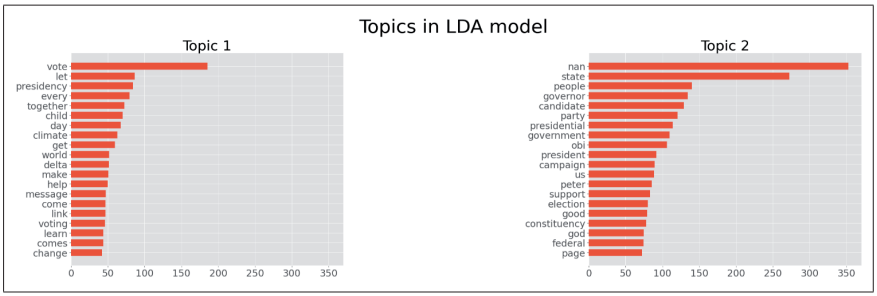

Figure 1: Word distribution of the two main topics discovered by LDA (Latent Dirichlet Allocation)

In Nigeria, based on the results presented in Figure 1, the topic model generated two primary topics; Topic 1 extended beyond the electoral campaigns to encompass socio-political matters while Topic 2 addressed concerns related to presidential candidates and their election campaigns with a particular emphasis on Peter Obi's candidacy. Although both topics centered on the Nigerian 2023 election campaigns, Topic 1 extended beyond the electoral campaigns to encompass broader socio-political matters, including development and education. Conversely, Topic 2 exclusively addressed concerns related to the presidential candidates and their election campaigns, with a particular emphasis on Peter Obi's candidacy. Topic 1 was subdivided into nine distinct subtopics, each addressing specific themes related to socio-political issues in the Nigerian 2023 election campaigns. The following table summarizes the subtopics and their corresponding focus areas:

Subtopic	Focus Area
1	Climate change issues
2	Maintaining peace during the election, health care, gender
3	Diseases related to nutrition and hygiene
4	Infrastructural development
5	Higher education and training
6	Petroleum and oil mining
7	Empowerment and development issues
8	Inequality and disabilities
9	Trust in government for a conducive environment for businesses

An analysis of Topic 2 reveals that it was subdivided into four subtopics. The first subtopic focused on galvanizing support for the presidential candidate Peter Obi and encouraging voter turnout. The second subtopic centered on promoting unity and peace during the elections to ensure a smooth transition of government, as well as highlighting the promises made by electoral candidates. The third subtopic mainly disseminated news and information on the campaigns and elections. The fourth subtopic addressed other global issues related to climate change, energy, COVID-19, and education. The subtopics and their corresponding focus areas are summarized in the following table.

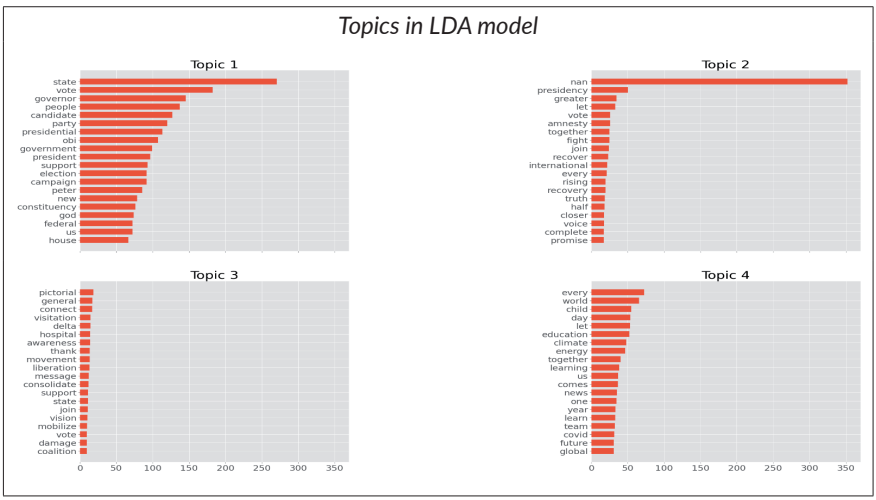

Figure 2: Subtopics for topic 1 uncovered by LDA.

i). Microtargeting

In addition to examining the descriptive statistics of the original dataset, the author conducted an upper-tailed test on the demographic and geographic variables, incorporating age and gender as demographic characteristics. Figure 3 illustrates the age distribution of the Nigerian election ads' target audience. It revealed that the ads did not specifically target any particular age group.

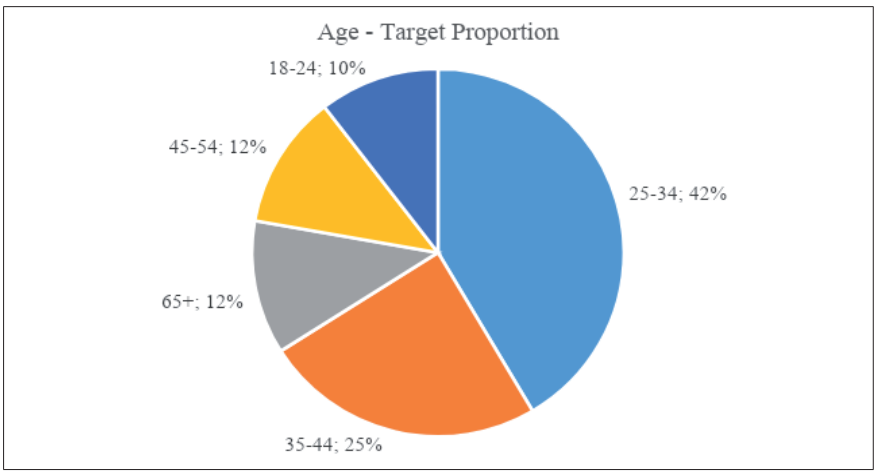

Figure 3: Age distribution of Ads

Nevertheless, the largest proportion of the target audience fell within the age range of twenty-five to thirty-four years. A fact check on Facebook usage in Nigeria during the ads' running period, March to August 2022, corroborates this finding, indicating that the largest Facebook user age group in Nigeria during that time was also between ages twenty-five and thirty-four years (NapoleonCat, 2022). Consequently, it can be inferred that no specific age group was targeted by the ads.

ii). Regional targeting

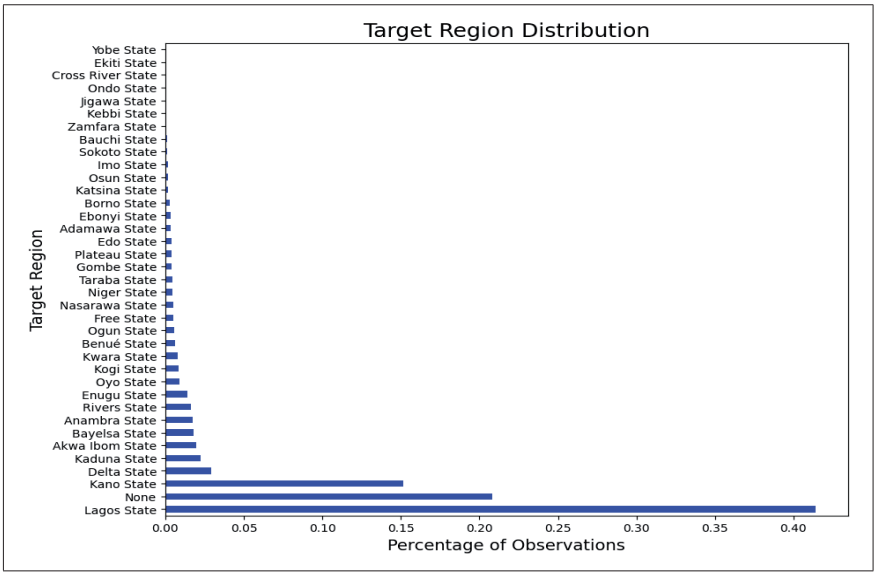

Figure 4: Regional targeting by political ads

Regarding the regional targeting, as presented in Figure 4, the majority of election ads were targeted toward Lagos during the 2023 election period, followed by 'None'. This suggests that Lagos state was the primary focus of the ads, while the remaining ads were shown to a more general audience. However, after conducting a fact check, it was discovered that Lagos has the highest number of Facebook users in Nigeria, accounting for forty-three percent (Thirteen million three hundred thousand million) of the country's Facebook users. Given this information, the study concludes that the ads were not specifically targeted toward particular regions but rather aimed at a broader audience.

The analysis of political ads during the Nigerian election revealed several important insights into the overall strategy and targeting approach. Similar to the findings in Kenya, the Nigerian ads did not specifically target any particular age group, although the largest proportion of the target audience fell within the age range of twenty-five to thirty-four years. This aligns with the demographic distribution of Facebook users in Nigeria

during the ad campaign period. Furthermore, there was no evidence of gender targeting in the Nigerian political ads, as the proportion of ads targeting each gender category was similar.

In terms of regional targeting, the majority of the ads were focused on Lagos, the state with the highest number of Facebook users in Nigeria. However, the analysis indicated that this was due to Lagos being a densely populated region and not necessarily a deliberate targeting strategy. The ads also reached a more general audience outside of specific regions, indicating a lack of specific regional targeting.

The content analysis of the ads reveals that the primary focus was on the messages and promises of electoral candidates, similar to the findings in Kenya. These ads accounted for a significant proportion of the content, indicating the importance placed on the candidates' campaigns and rallying for support. Other topics covered in the ads included education, COVID-19, development, and climate change, reflecting the broader issues and concerns during the election period.

Overall, the Nigerian political ads aimed to reach a general audience without specific targeting by age, gender, or region. The primary emphasis was on the electoral candidates' messages and promises, highlighting their campaigns and rallying for support. This aligns with the strategy observed in Kenya, where the focus was also on the candidates and their messages. The analysis provided valuable insights into the targeting approach and thematic content of political ads during the Nigerian election, shedding light on the strategies employed to engage the electorate.

However, it is important to note that while the study in Kenya and Nigeria does not reveal heightened political microtargeting at the moment, there is potential for this to occur due to the growing population of social media users and the migration of more political activities to the online space. Moreover, there is a trend to digitize voter registers in these countries as evident in the laws that this paper discusses in the subsequent part. Thus,

sophisticating the tool for potential microtargeting. Therefore, this study forms the basis for understanding the harms of political microtargeting and the applicable laws that could be activated to weather the storm.

IV. LEGAL ANALYSIS

This part outlines existing laws in Kenya and Nigeria that offer protection from the possible effects of political Microtargeting.

A. Existing laws applicable to microtargeting in Kenya and Nigeria

There is no specific legislation that addresses political microtargeting in both Kenya and Nigeria. However, it is crucial to determine whether both countries have the capability to curtail microtargeting practices in the absence of a single comprehensive law. The laws identified do not specifically mention the practice of microtargeting but the aspects that the laws address intertwine with the practice and therefore will be instrumental in regulation.

1. Kenya

i). The Constitution of Kenya, 2010

The Constitution of Kenya is the supreme law of the country. 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 (2001) 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 (Rubinstein, 2014).

The practice also threatens the political privacy of individuals by 'compromising the personal sphere' which is considered essential for democratic deliberation and self-determination (Rubinstein, 2014). Thomas Emerson (1970) 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'. Any breach of political data may stir certain ripple effects for instance voters may have 'diminished faith in publicly supervised political processes' (Rubinstein, 2014).

The provision on the right to privacy enshrined in the Constitution 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' (Rubinstein, 2014). 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 to fruition, the Data Protection Act was enacted into law in 2019 (Data Protection Act, 2019, preamble). 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 data is processed in accordance with the data protection principles provided for in the legislation (*Data Protection Act, 201*9, s 3(b)). Personal data should be processed with regard to the right to privacy of a data subject, in a lawful, fair, and transparent manner and should be collected for specified and legitimate purposes (*Data Protection Act, 2019*, s 25 (a), (b) and (c)). The personal data should also be relevant to what is necessary in relation to the purposes for which it is processed (*Data Protection Act, 2019*, s 25(d)).

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 (*Data Protection Act, 2019*, s 25(d)). 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 (*Data Protection Act, 2019*, s 2)).

When it comes to political microtargeting, two types of actors could be regarded as data controllers namely 'the online platforms and the political actors' (Casagran & Vermeulen, 2021). The Bavarian Administrative Court in 2018 held that Facebook and the user of the Audience should be considered joint data controllers *(VG Bayreuth, Beschluss v. 08.05.2018 – B 1 S 18.105)*. The Court of Justice of the European Union (CJEU) has also supported this idea *(Case C-210/16 Wirtschaftsakademie Schleswig-Holstein 2018)*.

One of the concerns of political advertising is the likelihood of violating the purpose limitation principle. The principle means that the collection of personal data should be for specific and legitimate purposes. Section 25 (c) of the Act provides that data processors must 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' (Bennett, 2016). 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' (Casagran & Vermeulen, 2021). This provision is key in restricting microtargeting practices since it places restrictions on the processing of personal data.

The data minimization principle also plays an important role in regulating political microtargeting. Section 25 (d) of the Act provides that the processing of personal data has to be 'ad-

equate, relevant, limited to what is necessary for 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 fulfill their purpose. It would also require 'periodic reviews of the data held with deletion of the data items that are no longer necessary' (Casagran & Veremeulen, 2021).

Consent is also required from a data subject before processing their personal data for a specified purpose (*Data Protection Act, 2019*, s 32(1)). The data belonging to a voter can therefore be collected for targeting and microtargeting purposes if they have given consent for it to be used for such purposes (Mude, 2021). 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 (*Data Protection Act, 2019*, s 37(1)(a)). 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 (*Data Protection Act, 2019*, s 31(1)).

Political microtargeting also involves profiling voters so as to influence their voting behavior. Profiling entails the evaluation of an individual's personal data to analyze or predict certain aspects of a person such as their habits, personality, political beliefs, and many other aspects (Privacy International, 2020). By analyzing the personal data, targeted political messages can then be sent to voters based even on their name since they identify someone's tribe and are 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…' (*Data Protection Act, 2019*, s 35(1)). Where a decision is made based on processing, the data processor is required to notify the data subject in writing (*Data Protection Act, 2019*, s 35(3)(a)). These provisions will

play a crucial role in regulating political microtargeting. They restrict data processors from engaging in the automated processing of personal data for profiling purposes without the explicit involvement of the data subject.

The legislation also provides for sensitive personal data and this kind of data includes a person's race, biometric data, and ethnic and social origin (*Data Protection Act, 2019*, s 2)). The ethnic origin of a person can easily be identified by the name one holds. This makes it easy for political actors to target certain individuals (Mude, 2021). 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 and one of the grounds for processing sensitive personal data provided for in Section 45 of the Act (Mude, 2021).

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 based on consent. A data subject will therefore be aware of the implications involved in processing personal data. Regulation 4 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 the kind of personal data collected.

Such measures will hinder political microtargeting since they will ensure transparency is observed and political actors do not misuse personal data that 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 could give consent (*Data Protection (General) Regulations*, 2021, Regulation 4(3)).

The Regulations also recognize 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...' (*Data Protection (General) Regulations*, 2021, Regulation 14(2)(b)). 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' (*Data Protection (General) Regulations*, *2021*, Regulation 15(1)(b)).

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' *(Data Protection (General) Regulations*, *2021*, Regulation 15(1)(c)). Direct marketing has the potential to be 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 (Cavaliere, 2021) Direct marketing is pivotal to the practice of political microtargeting since it involves sending of personalized communications to the data subject. Political campaigns are now using direct marketing to 'promote candidates and influence potential voters' (Cavaliere, 2021). With the above conditions in place, the Regulations will be essential in ensuring that personal data is handled appropriately before direct marketing takes place thus hindering the misuse of personal data for microtargeting purposes.

The right to object to processing is recognized in the Regulations and it is also applicable where processing is for 'direct marketing purposes which include profiling…' (*Data Protection (General) Regulations*, *2021*, Regulation 8(4)). If a data subject objects to the processing of his or her personal data for instance where it is obtained for political microtargeting purposes, he or she can request for erasure or destruction of the data *(Data Protection (General) Regulations*, *2021*, Regulation 12). The Regula-

tions 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 microtargeting practices.

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' *(Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021,* Regulation 3(1)). The Regulations play a key role as it provides a framework through which the Data Commissioner would register data processors and controllers. This includes political parties and candidates, thus, ensuring that the activities they engage in are monitored (Sugow & Rutenberg 2021). The Regulations provide that a data controller or data processor is required to register as a data controller or processor where personal data is processed for 'canvassing political support among the electorate *(Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021*, third schedule)'.

Political microtargeting involves many actors, for example, political advertisers, political parties, political consultants, online platforms, content service providers, data brokers, and data analytics companies (Casgran & Vermeulen, 2021). Data brokers may act as controllers or processors 'depending on the degree of control they have over the processing' (European Commission, 2019). 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 (Casgran & Vermeulen, 2021). European national data authorities and the Court of Justice of the European Union (CJEU) have supported the idea that social media companies that offer 'custom' audiences should be considered as joint controllers with the advertiser (*Case C25/17 Tietosuojavaltuutettu [2018]*).

Where political microtargeting does not involve online social media platforms, the political actors should be considered as sole data controllers (Casgran & Vermeulen, 2021). The registration of all the political actors regarded as data controllers or processors will play an essential role in the accountability of personal data use. If personal data is misused for political microtargeting purposes, the data processors can be traced, and 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 deals with information security and data storage. The commission is required to come up with mechanisms to ensure the confidentiality of data and measures to protect against attacks on election technology (*The Elections (Technology) Regulations 2017*, Regulation 14). These measures are important so as to protect voters' alphanumeric and fingerprint data from being misused for instance through political microtargeting.

The IEBC maintains that its database has not been hacked to date since its data storage is not centralized. This is because it uses primary and secondary servers (Muthuri *et al*., 2020). The Commission also confirmed that it has an external disaster data recovery site (Muthuri, Karanja, Monyango & Karanja, 2020) which is in line with the requirements provided in Regulation 25 of the Elections (Technology) Regulations (*The Elections (Technology) Regulations, 2017*, Regulation 25(1) (a)).

The security of election technology is important so as to avoid any breach on the election website that may cause personal data to leak thus being misused for political campaign purposes like political microtargeting (IDEA, 2019). The Regu-

lations also require any person or telecommunication network service provider that becomes aware of any election technology vulnerability to notify the Commission **(***The Elections (Technology) Regulations 2017*, Regulation 27(1)). Measures such as this guarantee adequate protection of data belonging to voters thus securing the data from misuse. An example of a voter data breach is what happened in Mexico where the names and addresses of eighty-seven million voters could be accessed through Amazon's cloud computing site (Bennet, 2016). Therefore, this law helps to curtail political microtargeting practices in Kenya.

vi). The Computer Misuse and Cybercrimes Act, 2018

One of the threats of political microtargeting 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' (Zuiderveen et al., 2018). The issue of misinformation is addressed in the Computer Misuse and Cybercrimes Act (Section 22(1)), and it makes it an offense to misinform an individual with the intent that the data relied on shall be acted upon. This provision helps to curtail the practice of microtargeting since it places restraints on the spread of false information targeted toward specified voters which if relied upon can misinform them.

Another threat of microtargeting is with regard to privacy and especially data breaches. Once a hacker realizes that there is a loophole when it comes to the protection of data belonging to individuals, they can access databases containing personal data and then misuse it (Zuiderveen *et al*., 2018). This offense amounts to unauthorized 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 unauthorized…' **(***The Computer Misuse and Cybercrimes Act, 2018*, s 14(1)). Prohibiting unauthorized access to

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 (Section 17(1)) makes it an offense to intentionally or without authorization intercept data and cause it to be transmitted to a computer system or telecommunication system. 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 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.

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, and 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 creation and maintenance of member registers.

On microtargeting, the Guidelines make provisions on the right not to be subject to automated decision-making. This provision states that voters have the right not to be subject to decisions significantly affecting them based solely on automated processing of data without having their views taken into consideration or without human intervention. Also, on automated decision-making, the Guidelines provide that when voters receive or are subjected to the automated delivery of digital political advertising, they have the right to know why they are receiving such advertising material or receiving the 'ads' (*Office of the Data Protection Commissioner, Guidance Notes for Electoral Purposes, 2022*).

2. Nigeria

Similar to Kenya, Nigeria lacks a specific law to regulate political microtargeting. Although, the country has several existing laws that can regulate practical aspects. Some of the laws and regulations that are applicable to the practice of political microtargeting include:

i). The Constitution of the Federal Republic of Nigeria (1999, as amended)

Like most jurisdictions, Nigeria's data privacy and data protection regime emanates from the fundamental legislation of the land, that is, the Constitution of the Federal Republic of Nigeria 1999, as amended ('the Constitution'), which, by virtue of Section 37 protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication. Data privacy and protection are extensions of a citizen's constitutional rights to privacy (The Constitution of the Federal Republic of Nigeria, 1999). Similar to Kenya, the Nigerian Constitution protects the political privacy of citizens and therefore the respective authorities have to come up with measures to protect the privacy of voters and this involves the negative impact of microtargeting like misuse of personal data that has been collected for other political purposes.

ii). Data Protection Act 2023 (hereinafter, the Act)

The Act was enacted into law in June 2023, and it aims to enhance data protection and privacy rights for all Nigerian nationals. This Act applies to the collection, storage, processing, and use of personal data for individuals residing in Nigeria or of Nigerian nationality, regardless of the means employed (Asuquo, 2019). The Act applies to data controllers or data processors domiciled, ordinarily resident or ordinarily operating in Nigeria or where the processing of personal data occurs within Nigeria. It also applies to data controllers or data processors not domiciled,

ordinarily resident or ordinarily operating in Nigeria, so far they are processing personal data of data subjects in Nigeria.

In line with Section 27 of the Act, the burden of proof for establishing a data subject's consent is on the data controller. It should be noted that the silence or inactivity by the data subject shall not constitute consent. The consent may be granted in writing, orally, or through electronic means. The data subject can also withdraw his consent at any time. It is important to note that the withdrawal will not affect the lawfulness of prior data processing (Asuquo, 2019).

The Data Protection Act 2023 establishes a comprehensive framework for protecting personal data, ensuring individuals have control over their information. It emphasizes the need for informed consent, purpose limitation, data minimization, security measures, and individual rights. The above conditions encapsulated in Section 24 and Section 25 of the Data Protection Act 2023 are crucial in regulating microtargeting campaigns, which often rely on personal data for tailored advertising and communication. From the examination of the Act, data controllers and data processors are given a higher responsibility to match the high level of accountability that is expected of any organization entrusted with the personal data of data subjects.

iii). Cybercrimes (prohibition, prevention, etc.) Act 2015 (CPPA)

This is the main legislation dealing with cybersecurity in Nigeria. The Cybercrimes Act provides an effective, unified, and comprehensive legal regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Cybercrimes Act promotes cybersecurity, the protection of critical national information infrastructure, computer systems and networks, electronic communications, data and computer programs, and privacy rights (*CPPA*, 2015).

The fundamental purpose of the CPPA is to establish a framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. Significantly, it requires such service providers to accord premium to an individual's right to privacy as enshrined in the Constitution and to take steps towards safeguarding the confidentiality of data processed (*CPPA*, 2015).

Certain provisions within the Cybercrimes Act have implications for political Microtargeting campaigns. For example, according to Section 38 of the Cybercrimes Act, service providers have a duty to retain records and protect traffic data for a period of two years, having due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria (1999) (*CPPA*, s. 38). The data retained by these service providers are accorded the Constitutional right to privacy enshrined in the constitution and the service providers are required by law to take all appropriate measures to protect such data (*CPPA*, s. 38). This principle requires personal data to be retained only for the period that the data is required and for the purpose for which it was originally collected and stored. The fact that the data controller has come across another use of the data cannot justify blanket or indefinite retention (Asuquo, 2019).

The CPPA also emphasizes the importance of protecting individuals' right to privacy, as enshrined in the Nigerian Constitution. It requires service providers to take steps towards safeguarding the confidentiality of the data they process. This provision aligns with the broader principles of data protection and privacy rights, which are essential considerations in political microtargeting campaigns. Section 6(2) of the Cybercrimes Act further makes it an offense for any person, without authorization, to access a computer system with the intent of obtaining computer data and securing access to any program, commercial or industrial secrets, or classified information. The offender upon conviction is liable to imprisonment for seven years or to a fine of not more than seven million Nigerian Naira, or both (Asuquo, 2019).

In conclusion, while the CPPA primarily aims to address cybercrime, certain data retention and privacy provisions have implications for political Microtargeting campaigns. The Act's requirements regarding storing and safeguarding subscriber information align with the broader principles of data protection and privacy rights.

iv). Internet Code of Practice

The Nigerian Communications Commission, in accordance with its authority to regulate the communications sector in Nigeria as expressed in the Nigerian Communications Act (2003), publishes the Internet Code of Practice to define the rights and obligations of Internet Access Service Providers with regard to the issues therein (Internet Code of Practice, 2022). The establishment and enforcement of the Code is envisioned as a co-regulatory effort between the Commission and industry stakeholders, hence the public consultation and incorporation of stakeholder feedback into the final document (Internet Code of Practice, 2022).

Section 4.2 of the Internet Code of Practice stipulates that an Internet access service provider shall take reasonable measures to protect customer information from unauthorized use, disclosure, or access. An Internet access service provider should consider the sensitivity of the data collected and the technical feasibility when implementing security measures (Internet Code of Practice, 2022).

Section 6 of the Code specifically discusses the Safeguards against Unsolicited Internet Communications. (Internet Code of Practice, 2022). Subsection 6.1 provides for the incorporation of Anti-Spam Policies into terms and conditions of service. Internet access service providers are required to include in their terms and conditions of service, rules prohibiting the use of the service to spam other users of the Internet. Also, the terms and conditions shall be published prominently on the internet access service provider's website and all service agreements, either electronic or otherwise.

v). The Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations 2011 (NCC Regulations)

Pursuant to Section 70 of the Nigerian Communications Act 2003 (*NCA,* 2003), the Nigeria Communications Commission hereinafter NCC is empowered to make and publish regulations concerning multiple subjects including but not limited to permits, written authorization, licenses, offenses, and penalties relating to communication offenses (Nigerian Communications Commission, n.d.). Drawing from this authority, the NCC issued the NCC Regulations which apply to telecommunications companies.

In the context of this study, there is a relationship between the National Communication Act 2003 (NCA), NCC Regulations, and political microtargeting. Regulation 9 of the NCC Regulations specifically addresses the rights of subscribers whose personal information is stored in the Central Database. It grants subscribers the entitlement to request updates, keep their data confidential, prevent duplication of subscriber information without authorization, and preserve the integrity of their information. These provisions align with the principles of data protection and privacy, which are crucial considerations in political microtargeting campaigns.

Additionally, Regulation 10 of the NCC Regulations stipulates that any release of a subscriber's personal information must be subject to the consent of the subscriber or in accordance with the provisions of the Nigerian Constitution, Acts of the National Assembly, or the NCC Regulations. This provision ensures that the disclosure of personal information in political microtargeting campaigns requires the explicit consent of the subscriber or compliance with legal frameworks.

By establishing these regulations, the NCA 2003 and the NCC Regulations provide a framework for protecting subscribers' personal information and ensuring its lawful and respon-

sible use. These provisions create safeguards against unauthorized access, misuse, or abuse of personal data, which is relevant in the context of political microtargeting campaigns. Thus, political microtargeting campaigns that utilize subscriber information must adhere to the guidelines set forth by the NCC Regulations. This includes obtaining consent from subscribers for data usage, maintaining data confidentiality, preventing unauthorized duplication of subscriber information, and complying with the provisions of the Nigerian Constitution and relevant Acts of the National Assembly.

vi). Electoral Act 2022

The recently implemented Electoral Act, which embraces technological advancements, has the potential to impact political microtargeting practices. The Act permits the use of electronic devices such as smart card readers and electronic voting machines during the voter accreditation process and throughout the elections (Eme, 2022). This integration of technology creates opportunities for political campaigns to gather real-time data and insights, enabling more precise microtargeting strategies. Moreover, the new Act introduces provisions for the electronic transmission of election results, following a procedure determined by the Electoral Commission (*Electoral Act*, 2022).

Also, the Act mandates the maintenance of the Register of Voters in electronic format within the central database of the electoral commission, in addition to manual or hardcopy formats (*Electoral Act, 2022*, Section 9(2). This digitalization of the voter register enhances data accessibility and accuracy, potentially enabling more effective microtargeting campaigns based on voter demographics, preferences, and behaviors. As a result, the Electoral Act's incorporation of technology not only modernizes the electoral process but also has implications for political microtargeting. The availability of real-time data and a digitalized voter register can provide political campaigns with enhanced tools and resources to refine their microtargeting strategies and en-

gage with specific segments of the electorate in a more targeted and efficient manner. This is a positive aspect of microtargeting while others include reaching voters at a personal level and it also prevents wastage of resources since only interested voters are targeted with the appropriate political messages.

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 microtargeting 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 digital sector will require legislators to enact laws addressing specific sectors being affected by technological advancement including the political arena.

V. 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 that deal with election matters. Political microtargeting is a separate practice that 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 actions in case an issue arises. The gap in the identified laws is that they

lack provisions addressing microtargeting as a unique subject or matter.

Several countries have come up with initiatives to regulate online political microtargeting and both Nigeria and Kenya can gain insights 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 instituted new transparency rules for elections. It also regulates campaign advertising through social media platforms such as Facebook, Google, and Twitter (Reepschlager & Dubois, 2019).

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 (*Elections Modernization Act 2018*, s. 206(2) amending s. 319 of the Elections Act)'. 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 (Pal, 2020).

The Canadian legislation gives an elaborate definition of what an online platform is and what it entails. The rapid internet growth in both Kenya and Nigeria has 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 both countries.

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: a registered or eligible party, a registered association, a nomination contestant, a potential candidate or a candidate; or a third party that is required to register under subsection 349.6 (1) or 353(1) (*Elections Modernization Act, 2018*, section 325.1(1)'. (Cwajg, 2020, p.14).

The owner or operator of the online platform is required to keep the information in the registry for five years to prevent the information from being destroyed when it is required urgently such as in cases of litigation or when there are 'investigations for breaches of the Elections Act' (Pal, 2020).

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 (Cwajg, 2020). In order to increase accountability, the record-keeping requirement can be included in both the Kenyan and the Nigerian election laws so as to simplify the public inspection process and also to identify the entities 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 (Cwajg, 2020).

The above provision is an example of the disclosure requirement that is fundamental in online political advertisement regulations. Disclosure requirements are important because they enable interested parties like the public and the media to inspect records that may be hidden from them (Ferguson, 2023). The requirement is also important because it provides details of the organization or individual's name that requested 'to place or paid for the advertisement' (Cwajg, 2020). This enhances the transparency of online political ads and also ensures that personal data is not misused. Having a similar provision in the electoral laws of both countries will enable voters to be aware of the individuals behind the advertisement and it will also complement the data protection laws 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 (Cwajg, 2020). 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.' The prohibition of commercial advertising is key in ensuring that voters are not swayed toward a particular political figure or party.

Additionally, in 2018 France introduced other rules under Article L.163-1 providing that three months before elections, online platforms should provide users with information about who paid for the 'promotion of content related to a debate of general interest' (Fathaigh & Borgesius, 2019). With the rapid increase of social media in both Kenya and Nigeria, information spreads fast. Politicians have also been accused of spreading election propaganda during the election period. By including a provision that requires social media platforms to provide details of individuals who placed or paid for the advertisements, it will expose the individuals behind the advertisements therefore minimizing the spread of political content meant to influence voters to vote in a specific way.

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 that cloud their freedom of choice (IDEA, 2018). 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.

Singapore has 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 the transparency of online political advertisements (Paragraph 4).' It defines what political advertisement entails (Paragraph 3(a)). 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 and Nigerian electoral laws since it will help to avoid ambiguity.

The Code also has a disclosure requirement for online political advertisements (Paragraph 6 (b). Furthermore, 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 organization who requested or paid to place the advertisement', must be kept and made available for viewing by the POFMA office' (Paragraph 6(c).

Just like in France and Canada, the disclosure and record-keeping provision plays a fundamental role in enhancing the

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 these requirements are among the key ones that should be considered when establishing a robust legislation.

In the United States of America (USA), some states have enacted 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...' (Cwajg, 2020). Also, under the Act in section 13-405 (B) (1), an online platform shall be made available for public inspection.

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...' (Cwajg, 2020). 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 social network sites. It is also easy to target voters using social network sites since many people share information on these platforms. Therefore, incorporating social networks or social media in the definition of an online platform will 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 the Social Media Disclose Act which are both from California, the New York Election Law Rules and Regulations amendments, the Vermont General Assembly amendment, Washington State Legislature amendments, and Wyoming State Legislature amendment.

In the Netherlands, the Dutch Code of Conduct Transparency Online Political Advertisements was published in 2021 to address election transparency issues and disinformation in the

digital sphere. (CounteringDISINFO, 2021). It also covers paid online political advertising (IDEA, 2022). In part 3.2 of the Code, political parties commit to 'refrain from psychological profiling for targeting purposes in online political advertising' (IDEA, 2022). Also, online platforms commit to 'develop and enforce relevant transparency mechanisms' concerning political advertising (IDEA, n.d.).

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 both countries and also included in the electoral laws to avoid the negative impact of microtargeting.

The proposed European Union regulation on the transparency and targeting of political advertising is another legislation that 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' (Proposal for a Regulation of the European Parliament and the Council on the transparency and targeting of political advertising). The proposed regulation defines what political advertising entails (Proposal for a Regulation of the European Parliament and the Council on the transparency and targeting of political advertising, Article 2(2) (a) and (b).

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' (Article 4). 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…'(Article 3(c).

Online political advertising regulations should include transparency of political advertisements as an important feature of online political advertising. This is because it provides clarity on advertisers, protocols, and spending (IDEA, 2020). Therefore, through transparency, people can know 'who is behind an ad and how much money parties and candidates invested in online advertising' (IDEA, 2020). It is important to have a transparency provision when formulating a law on microtargeting because people should know 'who is targeting them and why they are being targeted' (IDEA, 2020). Also, through transparency in data use, individuals can gain a greater understanding of the impact of online political advertising, especially researchers (IDEA, 2020).

The definition of political advertisement and disclosure of information relating to political advertising yet again feature in this proposed regulation. In the Kenyan and Nigerian contexts, the mentioned provisions can be factored in when creating 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 both countries can assess the provisions from different legislations and then formulate similar provisions that are applicable in their country's context.

VI. CONCLUSION

This study aims to shed light on the evolving nature of political campaigning in the digital age by exploring the intersection between political advertising policies and political microtargeting. A general overview of the research indicates that political microtargeting has indeed become a powerful tool in contemporary political campaigns, allowing political actors to deliver tailored messages to specific groups of voters based on their

demographic characteristics, preferences, and online behavior. For instance, the data illustrated that a majority of election ads during the campaign period were targeted towards Nairobi and Lagos, the regions with the highest number of Facebook users both in Kenya and Nigeria.

The analysis further explores the existing legal and regulatory frameworks governing political advertising in both countries and highlights the need for comprehensive and contextually relevant policy frameworks that address the complexities and challenges associated with political microtargeting. Political microtargeting is an emerging phenomenon and from the illustrations described in this study from other countries, legislators need to come up with robust laws addressing it. This is because it has its threats which if not addressed can have a negative impact on voters. The laws applicable in Nigeria and Kenya can only regulate the practice to a limited extent and not holistically.

In conclusion, this paper demonstrates that vagueness in guidelines and policies addressing microtargeting poses serious challenges to the integrity of future elections in both regions and the overall democratic landscape. As such, aside from this research contributing to the growing body of knowledge on the evolving landscape of political communication in the digital age, it also calls for further investigation by scholars into the topic in order to contribute to the existing collection of suggested policy recommendations.

REFERENCES

Borgesius F, Moller J, Kruikemeier S, Fathaigh R, Irion K, Dobber T and Bodo B. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review, 14*(1), 82-96. https://utrechtlawreview.org/articles/10.18352/ulr.420.

Clough J. (2010). *Principles of Cybercrime.* Cambridge University Press.

Cwajg C (2020). *Transparency Rules in Online Political Advertising: Mapping Global Law and Policy.* https://www.ivir.nl/publicaties/download/TransparencyRulesOnlinePoliticalAds2020.pdf.

Cybercrimes (prohibition, prevention, etc.) Act 2015 (CPPA) (Nigeria).

Data Protection Act 2023 (Nigeria).

Delacourt S. (2013). *Shopping for Votes: How Politicians Choose Us and We Choose Them*. Douglas& McIntyre.

Dobber T, Fathaigh R and Borgesius (2019). The regulation of online political microtargeting in Europe *Internet Policy Review* 8(4), 1-20.

Dorado, R., & Ratté, S. (2016). Semisupervised text classification using unsupervised topic information. *The Twenty-Ninth International Flairs Conference*. Duong, T. (2013). Local significant differences from nonparametric two-sample tests. *Journal of Nonparametric Statistics*, 25(3), 635–645. https://aaai.org/papers/210-flairs-2016-12894/

Electoral Act 2022 (Nigeria).

Guidance Note for Electoral Purposes (Kenya).

Hankey S, Morris J and Naik R. (2018). *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.

Hillygus D and Shields T. (2008). *The Persuadable Voter: Wedge Issues in Presidential Campaigns.* Princeton University Press.

ICNL. (2018). *The Legislative Dilemma.* https://www.icnl.org/wp-content/uploads/Disinformation-The-Legislative-Dilemma..pdf

Internet Code of Practice 2022 (Nigeria).

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. https://academic.oup.com/bioscience/article/51/5/341/243981

Lin E .(2002). *Prioritizing Privacy: A Constitutional Response to the Internet.* https://lawcat.berkeley.edu/record/1118208/files/fulltext.pdf.

Pariser E. (2012). *The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think*. Penguin Publishing Group.

Pasquale F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information.* Harvard University Press.

Privacy International. (2021). *Micro-targeting in Political Campaigns: A comparative analysis of legal frameworks.* https://privacyinternational.org/sites/default/files/2021-01/UoE_PI%20Microtargeting%20in%20policital%20campaigns%20comparative%20analysis%202021.pdf.

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. https://10.1097/00000542-200004000-00035

The Computer Misuse and Cybercrimes Act 2018 (Kenya).

The Constitution of Kenya 2010.

The Constitution of the Federal Republic of Nigeria (1999, as amended).

The Data Protection (General) Regulations 2021 (Kenya).

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

The Data Protection Act 2019 (Kenya).

The Elections (Technology) Regulations 2017 (Kenya).

The Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations 2011 (NCC Regulations).

Bennett C. (2013, June 15). *The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2279920.

Green D. (2013, September 1). *Do Negative Political Ads Work?* https://www.scientificamerican.com/article/do-negative-political-ads-work/.

Gorton W. (2016, February 5). Manipulating Citizens: How Political Campaigns' Use of Behavioural Social Science Harms Democracy. *New Political Science 38*(1), 61-80. https://www.tandfonline.com/doi/full/10.1080/07393148.2015.1125119.

Bennett C. (2016, December 10). Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law 6(*4), 261-275. https://academic.oup.com/idpl/article/6/4/261/2567747.

Endres K and Kelly K. (2017, September 25). Does microtargeting matter? Campaign contact strategies and young voters. *Journal of Elections, Public Opinion and Parties 28*(1), 1-18. https://www.tandfonline.com/doi/full/10.1080/17457289.2017.1378222.

Philippi J. (2017, October 16). *The Myths of Data-Driven Campaigning.* https://www.tandfonline.com/doi/full/10.1080/10584609.2017.1372999.

Kosinski M, Nave G and Stillwell D (2017, November 13). *Psychological target-*

ing as an effective approach to digital mass persuasion. PNAS 114(48), 12714- 12719. https://www.pnas.org/doi/10.1073/pnas.1710966114.

Bodo B, Helberger N and Vreese C. (2017, December 31). Political Micro-targeting: A Manchurian Candidate or Just a Dark Horse? *Internet Policy Review 6*(4), 1-13. https://policyreview.info/articles/analysis/political-micro-targeting-manchurian-candidate-or-just-dark-horse.

BBC. (2018, March 20). *Cambridge Analytica's Kenya election role 'must be investigated'.* https://www.bbc.com/news/world-africa-43471707.

Crabtree J. (2018, March 23). *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.

The Guardian. (2018, March 23). *Leaked: Cambridge Analytica's blueprint for Trump Victory*. https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

Livingston S and Lance W (2018, April 2). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication 33*(2), 122-139. https://journals.sagepub.com/doi/10.1177/0267323118760317.

Rubinstein I. (2018, April 26).*Voter privacy in the age of big data.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447956.

Muthuri R, Karanja M, Monyango F and Karanja W (2018, May 9). Biometric Technology, Elections And Privacy in Kenya. https://cipit.strathmore.edu/biometric-elections-privacy-kenya/.

IDEA.(2018,June).*Digital Microtargeting.* https://www.idea.int/publications/catalogue/digital-microtargeting>.

Pocyte A. (2018, September 23). *Online Political Microtargeting In the United States.* https://thesecuritydistillery.org/all-articles/online-political-microtargeting-in-the-united-states.

Accessnow. (2018, October 26). *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/.

Reepschlager A and Dubois E (2019, January 2). *New election laws are no match for the internet.* https://policyoptions.irpp.org/fr/magazines/january-2019/new-election-laws-no-match-internet/.

Bennet C and Lyon D. (2019, December 31). Data-Driven Elections: Implications and Challenges for Democratic Societies. *Internet Policy Review 8*(4), 1-16. https://policyreview.info/data-driven-elections.

Montgomery K and Chester J. (2019, December 31). The digital commercialization of US politics-2020 and beyond. *Internet Policy Review 8*(4), 1-23. https;// doi.org:10.14763/2017.4.773

Philippi J. (2019, December 31). Data campaigning: between empirics and assumptions. *Internet Policy Review 8*(4), 1-18. https://policyreview.info/

articles/analysis/data-campaigning-between-empirics-and-assumptions.

Lambe K and Ricks B. (2020, January 14). *The basics on microtargeting and political ads on Facebook.* https://foundation.mozilla.org/en/blog/basics-microtargeting-and-political-ads-facebook/.

Privacy International. (2020, April 30). *Why we're concerned about profiling and microtargeting in elections.* https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections.

Pal M. (2020, May 6). *Evaluating Bill C-76: The Elections Modernization Act.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572737.

Casagran C and Vermeulen M (2021, August 20). Reflections on the murky legal practices of political micro-targeting from a GDPR perspective. *International Data Privacy Law 11*(4), 348-349. https://doi.org/10.1093/idpl/ipab018

Sugow A and Rutenberg I. (2021, October 1). *Securing Kenya's Electoral Integrity: Regulating Personal Data Use.* https://www.theelephant.info/op-eds/2021/10/01/securing-kenyas-electoral-integrity-regulating-personal-data-use/.

Papakyriakopoulos, O. (2022, July 1). *Social media and microtargeting: Political data processing and the consequences for Germany.* Sagepub. https://journals.sagepub.com/doi/pdf/10.1177/2053951718811844.