JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
eISSN: 2788-6727 — Volume 1, Issue 1 (2021) p. 7-36.
https://doi.org/10.52907/jipit.v1i1.61

Political Micro-Targeting in Kenya: An Analysis of the Legality of Data-Driven Campaign Strategies under the Data Protection Act

Hashim Mude[*]

ABSTRACT

The 2013 general election marked the entry of data-driven campaigning into Kenyan politics as political parties begun collecting and storing voter data. More sophisticated techniques were deployed in 2017 as politicians retained the services of data analytics firms such as Cambridge Analytica, accused of digital colonialism and undermining democracies. It is alleged that political parties engaged in regular targeting and more intrusive micro-targeting, facilitated by the absence of a data protection legal framework.

The promulgation of the Data Protection Act, 2019, ostensibly remedied this gap. This paper analyses whether, and to what extent, political parties can rely on the same—or similar—

[*] The author is an Advocate of the High Court of Kenya and holds an LLB at the Catholic University of East Africa (Nairobi, Kenya), LLM at the University of Edinburgh and is currently a PhD candidate at the University of Edinburgh (United Kingdom).

regular targeting and micro-targeting techniques in subsequent elections. While regular targeting differs from micro-targeting as the latter operates at a more granular level, both comprise of three steps—collecting a voter's personal data, profiling them, and sending out targeted messages.

This paper considers the legality of each of these steps in turn. It finds that going forward, such practices will likely require the consent of the data subject. However, the Act provides for several exceptions which political parties could abuse to circumvent this requirement. There are also considerable loopholes that allow open access to voter data in the electoral list as well as the personal data of the members of a rival political party. The efficacy of the Data Protection Act will largely rest on whether the Data Protection Commissioner will interpret it progressively and hold political parties to account.

Keywords: Political Micro-Targeting, Data-Driven Campaigning, Data Protection Act, Voter Data, Data Subject Profiling

TABLE OF CONTENTS

1. INTRODUCTION

Data-driven campaigning and its attendant consequences on the health of a democracy were initially thought to be the concern of the Global North. No confounded algorithm or fancy number-crunching was going to affect Kenya's ethnic-based politicking. Deploying such tactics here would be an exercise in futility.

However, in the 2013 and 2017 general elections, the major political parties are alleged to have engaged in data-driven campaigning (Muthuri *et al.*, 2018, p. 5; Mutung'u, 2018, p. 11-12). The Jubilee Party engaged the services of the controversial data analytics firm, Cambridge Analytica, to help it with 'branding', though subsequent investigative journalism suggests this was a gross understatement as they were said to have profiled and micro-targeted voters based on their fears and needs (Moore, 2018). A year on from the exposure of the scandal, the Data Protection Act, 2019 (DPA) came into force. This paper explores whether the various alleged micro-targeting activities like those that occurred in the 2013 and 2017 general elections remain legal after the promulgation of the DPA.

The analysis commences by distinguishing between regular targeting and political micro-targeting. This is followed by a brief overview of justifications in the literature for regulating these practices. Finally, the paper analyses whether—and to what extent—the DPA has affected the legality of the methods of targeting and micro-targeting utilised in the previous elections. In considering the adequacy of the framework, relevant comparisons are made between the DPA, on one hand, and the European Union's

General Data Protection Regulations (GDPR), and the United Kingdom's (UK) Data Protection Act (UK DPA) on the other.

2. What is Political Micro-Targeting and Why Do We Care About It?

Political micro-targeting is the *piece de resistance* of data-driven political campaigning. It involves the collection of a voter's personal data, profiling them using that data, and thereafter sending out highly tailored political advertisements to them (Borgesius *et al.*, 2018, p. 82). Utilising data in political campaigning is not a novel concept in the Global North as political parties have long relied on techniques such as door-to-door canvassing to garner information on voters' preferences, which are then amalgamated with other sources to "build large data sets and email lists at national and local levels" (Dommett, 2019, p. 3).

The difference between this regular targeting and micro-targeting is that the latter takes audience heterogeneity into account. A political party that advertises in a particular neighbourhood because its data indicates it has a significant support base there is engaging in regular targeting. Micro-targeting on the other hand is much more granular and personalised and would take into account the different ideological commitments and personalities of its supporters within the neighbourhood. As Dobber (2019) notes, a voter whose chief concern is 'cheaper solar panels' would be targeted with a different message than one who wanted a "softer stance on immigration" (p.3). The following example cited by the UK Information Commissioner (ICO) is illustrative. A political party could conduct a poll that indicates increased spending on crime prevention is more positively received by single mothers with teenagers. It would then process data to identify the number of parents living in any town, narrow down how many of those are single mothers with teenagers and target them with a campaign message focusing on this issue (Burkell, 2019, p. 5).

This level of personalisation in profiling, which big data has made possible, enables political parties in the Global North to

collect and aggregate vast data from different sources including an increased "focus on mining social media platforms" (Dommett, 2019, p. 3). These activities are often facilitated by external firms of data experts such as the now infamous Cambridge Analytica. Cambridge Analytica is claimed to use psychographic profiling predicated on a 'five-factor personality model (including: openness, conscientiousness, extroversion, agreeableness, and neuroticism)' to create tailored ads meant to exploit voters' vulnerabilities (Burkell, 2019, p. 5). A member of the European Parliament somewhat tongue in cheek noted that these increasingly sophisticated tools have made it possible to "predict a person's beliefs, even before they have formed them" (Veld, 2017).

Allegations regarding political parties' use of data-driven campaigning in Kenya can be broadly grouped into two categories based on the level of sophistication of the targeting. The first group relates to the activities of Cambridge Analytica, which had created a detailed profile of Kenyan voters that included key national and local political issues, levels of trust in key politicians, voting behaviours, and preferred information channels (BBC, 2018 March 20). These allegations meet the definition of micro-targeting due to the granularity of the profiling, which took audience heterogeneity into account.

The second group comprises of the allegations that both major political parties 'micro-targeted' voters to encourage registration and turnout. A study found that voters were profiled based on their perceived political affiliation using alphanumeric data—potentially obtained from the voters' register—including their name and polling station (Muthuri *et al.*, 2018, p.5; Mutung'u, 2018, p. 11-12). Voters then received messages encouraging them to vote for a particular candidate. The study further indicates that 22% of respondents received messages that identified them by their first name (Muthuri *et al.*, 2018, p.5). This form of targeting was not particularly complex as it is arguable that Kenya's unique socio-ethnic background means that political affiliation can be inferred with reasonable precision from two data points on a voter; their name and polling station (Andreassen *et al.*, 2008; Wanyama,

2014).[1] Moreover, while some voters received messages addressing them by name, the rest of the contents were generic bulk messages sent out to every voter in the electoral district and therefore lacking the degree of personalisation present in the examples above. Labelling this as micro-targeting is therefore a misnomer.

It has long been argued that political micro-targeting is an existential threat to the functioning of a democracy as the very act of carving up, profiling and sending out different—and perhaps contradictory—political messages has the capacity to sow division, perpetuate disinformation and aggravate voter polarisation (Borgesius *et al.*, 2018, p. 82). The weaponisation of data in a country like Kenya with a recent history of ethnic violence is a concern that ought not to be taken lightly. Others take a more sceptical approach asserting that these claims are empirically unjustified. They contend that most political parties do not have the necessary expertise to engage in an effective micro-targeting campaign leading to a "gulf between the rhetoric and reality of data-driven campaigning" (Dommett, 2019, p. 4). There is certainly a temptation to oversell, overhype and catastrophise the effects of political micro-targeting (Vold & Whittlestone, 2019, p. 7).[2]

The sceptics could in turn be accused of short-sightedness. Political parties will not always be incapable, particularly in future. Part of a legislator's mandate is to anticipate harms and intervene before they materialise rather than wait idly for them to come to pass. Moreover, harm does not have to be in large proportions to be regulated. Even the more radical claims for intervention such as a total ban on micro-targeting can be justified on account of democratic majoritarianism and citizens' political rights. Political parties do not have a right to collect data without consent with a view of manipulating a voter (Muthuri *et al.*, 2018, p. 14).[3]

---

[1] In Kenya it is possible to infer a person's ethnicity from their name and the electorate have usually voted along ethnic lines see Recent literature indicates a greater shift towards issue-based voting.

[2] Particularly as the jury is still out on whether it is actually effective or is a mere marketing ploy by data analytics firms who are incentivised to tout the effectiveness of their wares.

[3] While there is no large-scale polling data on this a CIPIT survey indicates that seventy-four percent of people surveyed were opposed to 'unsolicited campaign messages'.

These practices should also be regulated because they harm individual privacy. Privacy has intrinsic and instrumental value as it promotes other goods including "autonomy, dignity, fairness, reputation, self-development, intimacy, and bodily integrity" (Vold & Whittlestone, 2019, p. 3; Solove, 2006). The practice of aggregating personal information and profiling can have a particularly deleterious effect on autonomy. Baker (2004)defines autonomy as a person's "capacity (including the necessary opportunities) to lead a meaningfully self-authored life without unnecessary or inappropriate frustration by others" (p. 220; Brison, 1998, p. 319). Using personal data to attempt to influence a person impinges on self-authorship. As Vold (2019) argues "if such influence is used in coercive and manipulative ways, this could threaten a person's ability to make independent decisions and form independent beliefs or values" (p. 4).

Even regular targeting harms individual privacy as collecting and aggregating personal information exposes a person to insecurity such as identity fraud (Solove, 2006, p. 515). Moreover, if people suspect that they are being monitored they will self-censor and inhibit their personalities (Solove, 2006, p. 493; Baker, 2004, p. 221). It is because of these potential harms, both to the State and the person, that it is worth interrogating their legality under the newly promulgated DPA.

3. The Legality of Data-Driven Campaign Strategies in the DPA Era

This part will examine whether the reported targeting and micro-targeting strategies utilised by political parties in previous elections remain lawful after the promulgation of the DPA. Both forms of targeting comprise of the same steps; collecting personal data, profiling, and thereafter sending out targeted messages. Each of these steps will be considered in turn. The analysis will—where relevant—refer to comparative best practices and suggest solutions to remedy identified weaknesses.

3.1. Processing that was Illegal Prior to the DPA

The purpose of this article is to examine whether the DPA has affected the legality of practices that were lawful prior to its promulgation. Therefore, the forms of data processing that were illegal before it came into force will not be considered.[4] This includes processing of personal data held by certain State entities such as the Registrar of Persons(Registration of Persons Act 2012, s. 14 (1), (k), (l), (m)),[5] and the use of State surveillance systems which are designated to investigate and prevent acts of terrorism to spy on and collect data on voters for political campaigning.[6]

The unlawful processing of personal data of voters from the private sector will also be excluded Mutung'u, 2018, p. 20). This includes banks and mobile network operators who are required by law to collect and store their customers' personal information (Proceeds of Crime and Anti-money Laundering Act 2012, s. 45; Kenya Information and Communications (Registration of SIM-cards) Regulations 2015, r. 5). The popular mobile banking service, M-pesa, does this through physical ledgers maintained by their agents, which contain a record of the transacting customers' personal information including their name, ID number and mobile phone number. Banks have long been under a common law duty to maintain their customers' confidentiality that includes both the nature and details of their transactions as well as their personal information (*Intercom Services Ltd & 4 others v. Standard Chartered Bank*, 2002). Mobile banking services such as M-pesa as well as credit reference bureaus and telecommunication companies (National Payment System Regulations 2014, r.42 (1)); Information and Communications Act 2011, s. 27A (2) (c)), are subject to strict confidentiality requirements—they can only divulge personal data with their customers written consent, a requirement which (as will

[4] This is not to suggest that they do not form an interesting study in their own right as the lack of enforcement of existing law is a subject worthy of further consideration.

[5] Unauthorised use or disclosure of information obtained under the Act is an offence Section 14 (1) (k), (l), (m), *Registration of Persons Act* (Act No. 12 of 2012). This will be further addressed by the Draft Data Protection (Civil Registration) Regulations, 2020 should they be enacted.

[6] Intercepting communications requires a court order and can only be done if it relates to an offence under the Act.

be noted) is more onerous than consent under the DPA, which can be unwritten.

With this in mind sub section ii below examines how the requirement of consent and its exceptions applies to political parties under the DPA. Subsections iii, iv and v will then consider how these requirements affect the legality of the strategies of collecting, profiling and targeting voters utilised in previous election campaigns.

3.2. The Requirement of Consent under the DPA and Its Exceptions

One commentator has polemically noted that in promulgating the DPA, Kenya adopted a 'copy and paste principle' from both the GDPR and the UK DPA (Malumbe, 2019; Ruternberg, 2019). Others have perhaps more diplomatically referred to it as "heavy borrowing" (Monyango, 2019).

The similarities between the DPA and these instruments is certainly striking with many provisions appearing to have been lifted verbatim from both. While it is tempting to score an easy point by deploring what appears to be lazy law-making, it can be argued that these other frameworks—while certainly far from perfect—are tried and tested and, therefore, there was no need to reinvent the wheel. Moreover, the office of the Data Protection Commissioner (DPC) is in its nascent stages, therefore lacking a track record of practices to reference from. These similarities allow us to make use of the guidance developed by the much older EU and the ICO on the application of the GDPR to shine some light on how some vague provisions of the DPA are likely be interpreted.

In order to process personal information, a data controller or processor[7] must obtain the consent of the data subject, which must be "unequivocal, free, specific and informed". Such consent must be given through an "affirmative action" and it is therefore on an opt-in basis (Data Protection Act 2019). The data controller bears the burden of proving that the data subject has consented to the

[7] Unless otherwise stated any obligations on data controllers will equally apply to processors.

specific purpose for which they are processing the data (Data Protection Act 2019, s. 32). A voter's data can therefore only be collected for targeting and micro-targeting if they are made aware of and give specific consent to such usage. Moreover, processing that is likely to lead to a "high risk to the rights and freedoms of a data subject"—which arguably includes micro-targeting—can only be done after carrying out an impact assessment (Data Protection Act 2019, s. 31). In future elections or referenda, political parties will have to abide by these requirements unless they can rely on the following exceptions under the Act.

3.2.1. The Legal Obligation Exception

Political parties can process data without consent where it is done to comply with a legal obligation (Data Protection Act 2019, s. 30 (b) (ii)). This exception is extremely narrow in its scope as it only allows the data controller to process the data for the specific purpose required by the legal obligation. Therefore, a political party cannot rely on it to process the data for an unrelated purpose such as micro-targeting (Data Protection Act 2019, s. 30 (2)).[8]

3.2.2. The Legitimate Interest Exception

This exception has also been lifted verbatim from the GDPR and the manner in which it is interpreted in that framework is prescient (Data Protection Act 2019, s. 30 (b) (vii)). Under the GDPR the 'legitimate interest' exception is regarded as the most flexible and applies where a party cannot meet the higher thresholds such as public interest (discussed below). A legitimate interest is defined as 'the broader stake that a controller may have in the processing, or the benefit that the controller derives—or that society might derive—from the processing' and includes "fraud prevention, enforcement of legal claims and exercise of rights such as freedom of expression" (Data Protection Working Party, 2014, a. 29).

[8] The section provides that 'further processing of personal data shall be in accordance with the purpose of collection' this is in line with the general principle of purpose limitation under Section 25 (c), (d) of the Act.

This legitimate interest must be weighed against the data subject's right to privacy. This balancing exercise is referred to as the principle of proportionality, which has emerged as the "leading framework for evaluating rights violations" (Khosla, 2010, p. 298) and is one of the general principles of EU law. It is effectively "a doctrinal tool for the resolution of conflicts between a right and a competing right or interest" (Möller, 2012, p. 710). The principle is ingrained in Kenya's Bill of Rights and all limitations of rights and fundamental freedoms are subject to it. Therefore, it is clear that, as is the case under the GDPR, a political party in Kenya that intends to rely on this exception must satisfy the proportionality test which can be divided into three distinct stages (Constitution of Kenya 2010, a. 24 (1) (a), (b), (c); *Okiya Omtatah Okoiti v. Communication Authority of Kenya*, 2018); *Jacqueline Okuta & another v. Attorney General*, 2017).

The first stage requires the political party to demonstrate it is "pursuing a legitimate objective". "Democratic engagement" would meet this threshold and so does its right to freedom of speech particularly as political speech lies at the core of the right (Barendt, 2005, p. 18). In the second stage they must show that the processing is 'necessary' to meet this objective and that it could not have achieved the goal through less privacy intrusive ways i.e. by obtaining the data subjects consent. The proximity between the two parties is relevant. Where data is collected from the voter directly, the political party had the opportunity to obtain their consent at the time of collection and they are therefore unlikely to satisfy this second stage. The proportionality test culminates in the "balancing stage" where the value gained by the controller in processing the data will be weighed against the harm caused to the data subject's right to privacy. The more intrusive to individual rights the form of processing is the more likely the balance will tilt in favour of the data subject. All stages must be passed in order for the processing to be considered proportional.

3.2.3. The Public Interest Exception

Political parties can also process data without consent where it is necessary in the public interest (Data Protection Act 2019, s.

30 (b) (iv) & (vi)).[9] This is another instance of 'heavy borrowing' from the GDPR and it is pertinent to discuss the context in which it originally appears briefly. The exception is couched in general terms and the GDPR suggests that member states ought to delineate the "specific processing situations" that qualify as "public interest" (EU General Data Protection Regulations 2016, a. 6 (2); Dörrenbächer & Mastenbroek, 2019, p. 70). The UK DPA which domesticates the GDPR lists several processing situations qualifying as legitimate interest including "an activity that supports or promotes democratic engagement" signifying that electoral campaigning could serve as a basis for processing data without consent (UK Data Protection Act 2018, s. 8 (e)). The importation of this GDPR provision in its generic form and the failure to set out the specific processing situations that qualify as public interest creates uncertainty that can be exploited by political parties to avoid the consent requirement. In the absence of certainty under the Act it is incumbent upon the DPC to provide clarity on what activities qualify as public interest and whether—and under what circumstances—political parties can rely on it to process personal data without the data subject's consent.

It is equally important for the DPC to clarify that even if political campaigning qualifies as a public interest, the specific processing situation must—as with the legitimate interest exception above—abide by the principle of proportionality i.e. it must be necessary for political campaigning. This means that processing a voter's data without their consent to ascertain whether they are interested in learning more about a politician's campaign may be allowable, but detailed psychographic profiling of the opposition's voters and targeting them with messages designed to suppress voting ought to fail a proportionality test.

3.2.4. Sensitive Personal Data

The DPA establishes a special category of data referred to as 'sensitive personal data' and sets out a list of the personal data that

[9] This exception appears twice. See Section 30 (b) (iv) and (vi) *The Data Protection Act* (Act No. 24 of 2019).

falls within it. There are two issues that stand out from this list. Firstly, unlike the GDPR, the DPA does not explicitly include political opinions under sensitive data (EU General Data Protection Regulations 2016, a. 9 (1)). It is unclear whether it is implicitly included through the reference to "beliefs and conscience" or whether these simply refer to religious or philosophical beliefs.

Secondly, there are many cases where it is possible to infer a person's "ethnic social origin" from their name (Andreassen *et al.*, 2008; Wanyama, 2014). It could therefore be argued that storing a person's name could amount to processing sensitive data. This situation is not unique to Kenya as the ICO faced a similar issue which they addressed by indicating it would not be appropriate to classify names as 'special category data in every instance', rather, such categorisation would only be required when the data was being processed *specifically* in order to profile and target a person based on their ethnicity (Information Commissioner's Office, n.d.). Therefore, a name can only be classified as sensitive personal data if a political party uses it to identify a voter by ethnicity and targets them on that basis. If a political party seeks to do so, it would have to satisfy the conditions for processing personal data discussed above in addition to at least one of the permitted grounds for processing sensitive personal data under the DPA (s. 45).

There are three grounds that are potentially relevant to political parties. The first allows them to process sensitive personal data where it "relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes" (Data Protection Act 2019, s. 45 (a (i)). This exception is limited and restricts disclosure of the data to any third parties without the consent of the data subject.

This provision is also borrowed—word for word—from the GDPR which imposes an additional requirement that ought to be considered by the DPC as they look to develop guidance in this area. The EU Commission (n.d.) has noted that in processing the data of its member or former member(s) the "purpose of the data collection should be specified at the time of collection". Although this additional requirement is not in the original provision, it has

been considered as applying by implication from the general principle of purpose limitation. As the DPA also provides for this principle (s. 25 (d)), the DPC could read in a similar requirement to ensure that political parties do not abuse this exception to process sensitive data for a non-exhaustive list of purposes without consent.

The second relevant ground is where "[t]he processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller of the data subject" (Data Protection Act 2019, s. 45 (c) (ii)) . The term rights rather than "public interest" or 'legitimate interest' which apply in the exceptions to the processing of personal data (discussed above) suggests a much stricter test. It indicates that political parties cannot get away with invoking general grounds of public interest and would have to demonstrate that they need to process the data to exercise specific rights.

However, this ground is unfortunately drafted in much wider terms than the equivalent provision under the GDPR (2016) as the latter specifies that the rights of the controller only relate to the 'field of employment, social security and social protection law' (a. 9 (2) (b)). Therefore, under the GDPR, political parties are only able to rely on this ground to process sensitive personal data relating to their employees, not voters. The more expansive provision under the DPA indicates Parliament's intention to allow this ground to be relied upon to process sensitive data for more purposes.

The final relevant ground is where the "processing relates to personal data which is manifestly made public by the data subject" (Data Protection Act 2019, s. 45 (b)). The term "manifestly made public" is not defined under the DPA or under the GDPR but the ICO has issued useful guidance that the DPC ought to be cognisant of noting that "it clearly assumes a deliberate act by the individual. It's not enough that it's already in the public domain—it must be the person concerned who took the steps that made it public" (Information Commissioner's Office, n.d.). The political party would therefore have to be satisfied that the data subject has deliberately made it public. Moreover, publishing to a narrow audience such as a social media post accessible by friends and

family will likely fail this requirement as the relevant test is 'whether any hypothetical interested member of the public could access this information'. Therefore, a political party could not rely on this exception to mine or scrape data from a voter's social media page (Information Commissioner's Office, n.d.). Sensitive personal data is useful towards building detailed psychographic models to enable more effective micro-targeting and is therefore extremely valuable for political parties. It is for this reason that the heightened protection it receives under the DPA is laudable.

I have relied on the GDPR, UK DPA and guidance on their application to shed some light on how uncertainties and gaps in the DPA could be understood and have provided good reasons for doing so. However, it is important to concede that the DPC could interpret these provisions—and any others—quite differently from how they have been applied in comparable instruments, even where the DPA uses the same wording.

3.2.5. Collecting Voter Data

Collecting voter data is the first and most important aspect of micro-targeting. It lays the foundational bricks for the subsequent steps. If micro-targeting was a metaphorical snake, data collection would be its head. Without sufficient data, profiling and targeted messages are impossible. It is for this reason that the principal strategy against micro-targeting is to simply to make it harder to gather people's data (Dommett, 2019, p. 13). The bulk of my analysis will therefore be focusing on this step.

Subsection 3.2.5.1 examines the practice of collecting data from the register of voters which acts as a spine upon which political parties build through collecting data from other sources. This is followed in 3.2.5.2 and (3) by an analysis of methods of direct collection of personal data. 3.2.5.4 and (5) discuss forms of indirect collection of voter data including from obtaining the membership lists of a rival political party and purchasing data from third parties such as data brokers. Finally 3.2.5.6 and (7) consider steps typically taken by parties after collecting the data.

3.2.5.1. Access to the Register of Voters

In many countries political parties and candidates are granted access to the register of voters (voter list) and this is justified on the ground that it helps them communicate with voters, furthers political debate and "promotes democratic participation" (Information Commissioner's Office, n.d.). There is certainly a legitimate interest for political parties to know the number and general location of registered voters as this informs them where they should allocate their finite campaign resources (Bennett, 2016, p. 269). A political party that does not have this information runs the risk of racking up inefficient expenses such as placing billboards in a location with no (or a few) registered voters.

The voter list in Kenya is a public record that can be accessed online during the election period (Elections Act 2011, s. 6). It can also be acquired during any other period by any person via a request under the Access to Information Act (Muthuri *et al.*, 2018, p. 15). As it is a public record the right to access and process the personal information within it is exempt from the consent requirements under the DPA. Parties can therefore collect and process the personal data within the list without the consent of the data subject (Data Protection Act 2019, s. 28). The personal data within it includes the voter's name, electoral area and—since at least 2010—a partially-redacted national ID number. The electoral management body (EMB), the Independent Electoral and Boundaries Commission (IEBC), has argued that redaction is necessary in order to balance "the right of information of third party's vis-a-vie the right of the voter to privacy of their personal identification details" (*Orange Democratic Movement (ODM) Party v. IEBC,* 2019). However, this policy was successfully challenged in *Orange Democratic Movement (ODM) Party v IEBC* where the court ordered the EMB to publish an unredacted voter list containing the voter's ID numbers for use in a by-election. The decision was predicated on an unelaborated distinction between an ID number—which was treated as non-confidential—and confidential information such as "telephone numbers, home or property searched, possessions seized and information relating to their family or private affairs unnecessarily required or revealed or

privacy of their communication" which can be injurious to a voter if released to the public (*Orange Democratic Movement (ODM) Party v. IEBC,* 2019).

This categorisation of an ID number as non-confidential and not injurious if made public does not reflect reality as it fails to account for the omnipresent role of the national ID in Kenyan life. It is a personally identifiable number and is a pre-requisite to access most Government services such as passport acquisition, land registration, public healthcare as well as utilities such as electricity and water and a plethora of private sector services including access to mobile networks and banking. It is routinely requested to allow entry into most Government and even privately-owned buildings. Possession of an individual's ID number could facilitate identity fraud and can, if keyed into certain databases, lead to the disclosure of sensitive personal information (Caribou Digital, 2019; Mutung'u, 2018, p. 9). Therefore, the court could be accused of failing to pay sufficient attention to the significance of allowing unfettered access to the ID number of every voter. While the ramifications of this decision on future elections is far from clear, it would seem that going forward any person can request and expect to receive an unredacted voter list from the IEBC.

The accessibility of this document has clear implications on the ease of micro-targeting the voting populace, which is often conducted by specialist data analytics firms as is evident from the Cambridge Analytica scandal. In Kenya they can directly acquire the voter list to build their databases for profiling and whereas only a citizen can make an access request (*Access to Information Act* 2016, 4(1) they are not barred from subsequently transmitting the information they acquire to any person including foreign entities. It is this kind of 'data neo-colonialism' that is facilitated by the absence of controls on access to the voter list (Madowo, 2018, n.d.).

In contrast to this approach, countries with strong data protection laws have taken steps to limit both who can access and what a voter list can be used for. For example, Canada (General Data Protection Regulation (GDPR); Standing committee on access

to information, privacy and ethics, 2018)[10] limits access to the list to political parties and candidates who can only use the information to communicate with voters. While they can theoretically engage third parties to process the data, they remain the controllers. Using the data for any other purpose is a criminal offence and a third party cannot therefore misappropriate the voter list to build its own databases or engage in political micro-targeting on behalf of any other entity as it has no entitlement to the data in its own right (Elections Act 2000, Canada, s. 111 & 487 (1) (b)). This ensures that political parties are accountable for how the data in the list is used.

The UK adopts a more nuanced approach and splits the voter list into a full and an open register with differing rights of access. The full register contains the names and addresses of every registered voter. Only political parties, candidates as well as Government departments and credit reference agencies can access the full register. Secondary legislation limits the use of the personal information within it to specific purposes and prohibits sharing it with other entities (Representation of People Regulations, England & Wales, r. 102 (6)). The open register on the other hand contains the names and addresses of those who have not opted out of it when registering as a voter. It can be purchased by any person on the payment of the requisite fees (Representation of People Regulations, England & Wales, r. 102 (6)). This approach is a middle ground as it applies the restrictive Canadian model to the full register and the laissez-faire Kenyan model to the open register. Therefore, while third parties can appropriate and use the data in the open register for any purpose, the voter has a right to remove their name from it without affecting their right to vote, a choice that is unavailable to a Kenyan voter.

Moreover, the ID number that IEBC is now legally mandated to release is, as noted above, far more sensitive than any information contained in voter lists availed to political parties in either the UK or Canada. This dangerous combination of a near unfettered access to the register, a lack of controls on usage as well

[10] Canada provides a useful benchmark here as it is listed as an adequate third country under the GDPR and has a well-developed and transparent electoral system that has been regarded as less conducive to micro-targeting.

as the sensitivity of the information disclosed creates an environment that is substantially more conducive to micro-targeting than countries with good data protection practices.

A possible solution is to reconsider the status of the voter list as a generic public record comparable to any other information held by public entities, which can be requested under the Access to Information Act. In the jurisdictions mentioned above, access to and use of the voter list is governed by election-specific regulation, which is more precise and contextualised than general access to information laws. A second solution that does not involve an overhaul of the existing framework would be for the IEBC to rely on the ground of "unwarranted invasion of the privacy of an individual" (Access to Information Act, s. 6 (1) (d)), under the Access to Information Act to only allow a limited class of persons to access the list such as political parties and candidates though their ability to redact the ID number seems to have been curtailed by the court clearly.

3.2.5.2. Direct collection from Political Party Members to Compile the Membership List

In order to avoid politicking along ethnic lines, Kenya's Constitution requires political parties to have a "national character" (Constitution of Kenya 2010, a. 91). To operationalise this requirement, the Political Parties Act imposes certain conditions for registration including the recruitment of a minimum of one thousand members who reflect "regional, ethnic diversity, gender balance and representation of minorities and marginalised groups" (Political Parties Act 2011, s. 7). They are therefore required by law to profile their members to ensure these diversity requirements are met and thereafter collect and submit a list to the Registrar of Political Parties (Registrar) that includes the 'name, addresses and identification particulars' of *all* their members (Political Parties Act 2011, s. 7 (2) (f) (i)). It has been suggested that the imposition of this requirement triggered the mass collection and storage of voter data by political parties from 2012 onwards. As of 2016, it is reported that the ODM alone had registered around three million new members (Mutung'u, 2018, p. 21). As this

collection is mandated by law it is doubtful whether the members would have been aware that a political party could—at least before the promulgation of the DPA—use this data for other purposes such as micro-targeting lawfully.

Under the DPA, the default position is that the political party would require the consent of the member to collect their personal data. However, it could rely on the legal obligation exception to process it without consent for the specific purpose required by law i.e. for submission to the Registrar, processing for any other purpose would require consent (Data Protection Act 2019, s. 30 (2)).[11] The political party cannot therefore rely on this exception to use the personal data for micro-targeting. There are of course legitimate concerns raised by the fact that this data has already been collected and it is difficult to know whether the parties are misappropriating it for other purposes, but these are issues of transparency and enforcement and the point as to the illegality of such a practice still stands.

The 'legitimate interest' and the vague 'public interest' exceptions are also likely to be inapplicable as the political party would probably fail the second stage of the proportionality test. This is because such collection is not necessary to meet the legitimate objective as the political party has an opportunity to process the data in a less rights intrusive manner i.e. by obtaining the consent of the data subject when it is compiling the membership list. The purpose of processing the data will also be factored into the analysis in the balancing stage. Purposes that are particularly intrusive to individual rights such as micro-targeting will see the scales tipped in favour of the data subject. Moreover, where sensitive personal data is collected, the political party would also have to demonstrate that they meet one of the permissible grounds discussed above.

[11] The section provides that 'further processing of personal data shall be in accordance with the purpose of collection' this is in line with the general principle of purpose limitation Section 25 (c), (d).

3.2.5.3. Direct Collection from Other Voters: Door-to-Door Canvassing

The data in the voter list and membership list acts as the 'spine' that political parties build on through collecting and adding more granular information (Information Commissioner's Office, p. 51). This additional data can be obtained from the voters directly through activities such as door-to-door canvassing. Reports suggest that a significant amount of data collected in the 2013 and 2017 was sourced directly from the voters by grassroots campaigners and agents (Mutung'u, 2018, p. 20). Prior to the promulgation of the DPA, this collection was perfectly legitimate and could be done without disclosing to the voter what the political party intended to use the data for. This data could also be lawfully shared with third parties for processing and potential micro-targeting. Such practices have now been rendered unlawful unless the political parties obtain the consent of the voter—or where the exceptions discussed above apply—and where such consent has been obtained, the political party cannot process the data for unrelated purposes further.

3.2.5.4. Indirect Collection of Voter Data from Third Parties

It has been alleged that political parties have been collecting voter data from data brokers and building entry data indirectly (Mutung'u, 2018, p. 22-23). Purchasing of data from brokers is unlawful without the data subject's consent, which ought to be obtained by the initial controller and must be specific to the processing by the political party. The initial controller cannot rely on consent given for another purpose to further process the data for unrelated activities (Data Protection Act 2019, s. 30 (1) (a), (2)). A furniture store cannot therefore piggyback on consent given by their customer to process their personal data for direct marketing to then further process it for political campaigning either by itself or through selling it to a political party. While the conditions for obtaining consent for such further processing will likely be clarified by the DPC, comparative practices suggest that it ought to be extremely specific because it is a use of personal data that cannot be reasonably contemplated by the data subject. The ICO suggests

that general phrases such as "for political campaign purposes" are insufficient and the initial consent must name the specific political party (Information Commissioner's Office, p. 58).

The collection or purchase of data that buildings collect to enhance their security for political campaigning equally falls under this paradigm. In Kenya, it is common practice for both public and private entities to maintain physical ledgers containing the names, ID numbers, telephone numbers and entry and exit times of visitors (Mutung'u, 2018, p. 21). As this data is collected under the guise of building security, it cannot be processed for political campaigning lawfully. There was no oversight on the security of these records initially—but this is likely to change with the introduction of registration requirements for data controllers or processors, although the thresholds for mandatory registration will be set by the DPC (Data Protection Act 2019, s. 18 (1) (2)).

3.2.5.5. Indirect Collection from Public Records: The Curious Case of the Membership List

Indirect collection of personal data from public records remains legal and is exempt from the consent requirements under the DPA (s. 28 (2) (a)).[12] One of the areas that this exemption produces strange outcomes is in relation to processing of personal data from the membership lists submitted to the Registrar under the Political Parties Act. Once a political party lodges this list, the Act, the regulations and the guidelines provide that the Registrar shall hold it as a public record which any person can inspect and obtain a copy of (Political Parties Act 2011, s. 34 (d); Office of the registrar of political parties, 2014, p. 10).

This gives rise to a comical double-standard where the political party which collects the data directly from its members is required to obtain their consent to use it for purposes other than registration, but any third party—including rival political parties or any other bad-faith actor—can simply waltz in and process it

[12] Data from the register of births, marriage, deaths adoptions, persons etc are not public records and their processing is not exempt from the DPA. Draft regulations to provide for the terms under which they will be accessible under the Act have been published see Draft Data Protection (Civil Registration) Regulations, 2020.

without consent once it is lodged with the Registrar. This data, which includes the personal information of all the members of a political party can be particularly useful for micro-targeting to suppress its voters. The oft-cited example of this is the Donald Trump campaigns micro-targeted advertisements reminding African-Americans of his opponent's remarks referring to African-American males as 'super predators' to depress their turnout (Borgesius *et al.*, 2018, p. 87). Similarly, in Kenya, there were reports that, during the 2017 general election, voters were targeted with what has been described as an 'apocalyptic' advertisement titled 'Real Raila' that portrayed the main opposition candidate as a "dangerous, racist xenophobe" (Mutung'u, 2018, p. 41; Kelly, 2017). A repeat of this would be facilitated by the ease of access to the membership list.

The requirement to register members of a political party is not unique to Kenya as even a country such as Canada which has strong data protection laws imposes similar requirements. However, there are important differences that make the latter more protective of personal data. Parties in Canada need only disclose the personal information of 250 members rather than the entire list and third parties have no right to access it (Elections Act 2000, Canada, s. 385 (2) (i)). However, the more common practice is similar to that adopted in the UK where only the governing body and heads of the parties are registered and therefore the divulgence of membership list to the public is not an issue that is even contemplated in such a framework.

The process of registering political parties ought to be overhauled to match—or to at least be brought closer to—the more privacy enhancing practices in other jurisdictions. This can be achieved through applying the principle of storage limitation, which is an internationally recognised principle of data protection that requires personal data to not be stored after fulfilling the purpose for which it was processed (Data Protection Act 2019, s. 25 & 41 (3) (c).[13] Under the Political Parties Act (2011), the only listed

[13] While the principle of purpose limitation is not explicitly listed under Section 25, *The Data Protection Act* (Act No. 24 of 2019) it is implicitly incorporated through S. 25 (g) and (Section 41 (3) (c).

purpose for processing the data is for the Registrar to ensure that political parties meet the conditions for registration after which there would be no justification in retaining the data as a public record. This is supported by the fact that falling below the membership threshold, failing to maintain ethnic diversity or gender balance is not a ground for deregistration under the Act (s. 21). Therefore, the Registrar can prevent third parties from obtaining the personal data on the membership lists by disposing of it after confirming the requirements are met, only retaining information about the political party itself such as its registered office, accounts and personal data of the members of its governing body. Moreover, the Registrar's guidelines allowing inspection of the list by the public are soft-law instruments that can be revised to bring them in line with the spirit of the DPA.

3.2.5.6. Profiling Voters

Profiling is the second step of any data-driven campaign. It consists of analysing the data collected about an individual to predict their preferences and behaviour and classify them into groups such as people who watch a particular TV show or read a certain newspaper. The more numerous the data points collected the more effective profiling is. Profiling is therefore hindered in jurisdictions that make it difficult to engage in large-scale collection of personal data (Dommett, 2019, p. 13).

As noted previously, there are two distinct allegations of voter profiling that occurred in the previous elections. The first was the regular targeting reported by CIPET to encourage registration and turnout. This kind of profiling was fairly unsophisticated and was merely geared towards identifying the voter's political affiliation (Muthuri *et al.*, 2018, p. 5-6). Such profiling would no longer be lawful in future campaigns unless the requisite consent is obtained or where it is specifically allowed by law.

The second relates to Cambridge Analytica and the allegations that they created a sophisticated and detailed profile for micro-targeting Kenyan voters that included "[k]ey national and local political issues, levels of trust in key politicians, voting behaviours/intentions, and preferred information channels" (BBC,

2018 March 20). It is worth noting that Cambridge Analytica has been accused of 'overselling' its capabilities and it is prudent to maintain a sufficient degree of scepticism as to the veracity of their claims (Osborne, 2018 March 18). However, should their claims prove to be baseless, others may execute similar tactics in the future effectively, and it is important to consider what tools are available under the DPA to protect Kenyan voters should such factors re-occur.

As with the first allegation, the data subject would have to consent to such profiling. The kind of profiling used in micro-targeting is significantly more intrusive to privacy than that used for regular targeting because it reveals more information about a voter's personality. Such profiling will likely trigger the additional obligations under the DPA (s. 35(3)), which require the processor to notify the data subject that the profiling has occurred. The data subject then has an absolute right to object to such profiling—even where they had previously consented to it.[14] Once alerted, the data subject can also contest profiling, which has led to the inferring of inaccurate information about them that is more likely to happen when more ambitious psychographic models that seek to infer personality traits are utilized (Data Protection Act 2019, s. 34 (1) (a)). These additional requirements act as significant bulwarks against profiling for micro-targeting.

3.2.5.7. Sending Out Personalised Messages

Once data has been collected and the data subject profiled to predict their personality and preferences, the political party would then send them a personalised message. The underlying—but contestable—assumption is that the greater the congruence between a message and a voter's personality traits the more effective and persuasive it is (Krotzek, 2019, p. 3612). For example, if a voter's profile indicates that their primary political concern is endemic corruption then a message that focuses on combatting it may be more persuasive than a generic campaign message.

[14] The right under this Section is absolute unlike the general right to object (under section 35 of The Data Protection Act), which can be overridden by the legitimate the interests of the data controller.

However aside from the fairly opaque activities by Cambridge Analytica there is no indication that such sophisticated targeting was deployed in Kenya.

According to the survey, the targeted messages sent out by political candidates consisted of simplistic profiles and were largely generic containing the voter's personal information such as name and polling station. Only four percent of the respondents surveyed said that they had provided their contact details to the political parties suggesting that they could have been obtained through any of the non-consensual methods discussed above (Muthuri *et al.*, 2018, p. 9-10).

The DPA does not make reference to political communication but regulates it in line with other forms of data processing discussed above. A political party would be required to disclose—and obtain consent—for each purpose they intend to use the data. If a political party intends on collecting the data for profiling and direct marketing both these purposes must be disclosed and approved by the data subject. Similarly, as with profiling, personalised messaging that is particularly intrusive entitles a data subject to an absolute right to object to such processing.

While the right to object is certainly novel, the consent of the data subject for political communication was already required under the Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks (CA Guidelines) (2017 July, para. 10.1). Therefore, sending unsolicited political messages was illegal before the DPA, which has simply placed this requirement on a statutory footing.

In some ways, the CA Guidelines go even further than the DPA as they contain provisions on transparency, requiring political parties sending out political messaging through Bulk SMS and MMS to only do so through licensed content service providers. In order to send a political message, a candidate must make a formal request accompanied by the verbatim content, a signed letter by the sender approving its contents, and a copy of their ID (CA Guidelines 2017, para. 7). The message itself must bear the name of the sender or the political party (CA Guidelines 2017, para. 8).

However, these obligations do not apply to political communication on social media platforms and this means that bad-faith actors can avoid them by channelling their advertisements through these platforms. A similar problem was tackled in Canada by requiring online platforms to create a publicly available registry of all electoral advertisements published on their websites containing a copy of the message and the name of the person who authorised it (Elections Act 2000, Canada, s. 325 (1), (2), (3)).

4. CONCLUSION

This paper has explored whether political targeting and micro-targeting was legal during the general elections of 2013 and 2017, and whether that remains the case after the promulgation of the DPA. It has been argued that the introduction of an opt-in mechanism for processing personal information means that most of these practices have likely been rendered unlawful. However, the public interest exception is framed in broad terms and can be abused to circumvent this requirement. It has also argued that there are significant concerns raised by the accessibility of the data in the voters' and membership lists of political parties, which are not solved by the DPA and which require urgent remedial measures as these records contain sensitive information about voters including their ID numbers.

Ultimately, the DPA has the potential to revolutionise the way personal information is collected and used in political campaigning in Kenya. If well implemented, it can operationalise the constitutional right to privacy and disrupt the intrusive data practices of political parties. If not, the practice around data in Kenyan politics will not change. The stability and progress of our budding democracy may well be dependent on the office of the Data Privacy Commissioner.

REFERENCES

Access to Information Act, n.31. (2016, Kenya).

Andreassen, BA., Barasa, T., Kibua & Tostensen, A. (2008). "I acted under a lot of pressure": the Disputed Kenyan 2007 general election in context, NORDEM Report.

Baker, E. (2004). Autonomy and informational privacy, or Gossip: The central meaning of the first amendment. *Social Philosophy and Policy, 21 (2).*

Barendt, E. (2005). F*reedom of Speech*. Oxford University Press.

BBC. (2018, March 20). Cambridge Analytica's Kenya election role 'must be investigated.

Bennett, C. (2016). 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).

Borgesius, F. *et al.* (2018). Online political microtargeting: promises and threats for democracy. *Utrecht Law Review, 14(1).*

Brison, S. (1998). 'The Autonomy Defense of Free Speech. *Ethics, 108(312).*

Burkell, J. (2019). Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy. *Internet Policy Review, 8(4)*.

Caribou Digital. (2019). Kenya's Identity Ecosystem.

Constitution of Kenya (2010).

Data Protection Act, n.24. (2019, Kenya).

Data Protection Working Party. (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014), 24-25.

Dobber, T. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4).

Dommett, K. (2019). Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns. *Internet Policy Review,* 8(4).

Dörrenbächer, N. & Mastenbroek, E. (2019). Passing the buck? Analyzing the delegation of discretion after transposition of European Union law. *Regulation and Governance,* 13.

Elections Act (2000, Canada).

Elections Act, n.24. (2011, Kenya).

EU Commission. (n.d.). Commission guidance on the application of Union data protection law in the electoral Context (COM(2018) 638 final).

General Data Protection Regulation (GDPR). (n.d.).

General Data Protection Regulations 2016, EU 2016/679.

Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Network (CA Guidelines) (2017, July).

Information and Communications Act, c. 411A (2011, Kenya).

Information Commissioner's Office. (2018, July 11). *Democracy disrupted? Personal information and political influence,*

Information Commissioner's Office. (n.d.). What is special category data?

Intercom Services Ltd & 4 others v. Standard Chartered Bank (2002) eKLR.

Jacqueline Okuta & another v. Attorney General & 2 others (2017) eKLR.

Kelley, K. (2017, December 14). US media firm targeted Raila Odinga with attack ads, report says. Nation Africa.

Kenya Information and Communications (Registration of SIM-cards) Regulations (2015).

Khosla, M. (2010). Proportionality: An Assault on Human Rights?: A Reply. *International Journal of Constitutional Law, 8 (2).*

Krotzek, L.J. (2019). Inside the Voter's Mind: The Effect of Psychometric Microtargeting on Feelings Toward and Propensity to Vote for a Candidate. *International Journal of Communication*.

Madowo, L. (2018, March 21). How Cambridge Analytica poisoned Kenya's democracy. Washington Post.

Malumbe, O. (2019, November 27). Kenya's Data Protection Act still way off the mark. The Standard.

Möller, K. (2012). Proportionality: Challenging the Critics. *International Journal of Constitutional Law, 10(3).*

Monyango, F. (2019). Kenya: Overview of the Data Protection Act, 2019. Data Guidance.

Moore, J. (2018, March 20). Cambridge Analytica had a role in Kenya election, too. *New York Times.*

Muthuri, R., Karanja, M., Monyango, F. & Karanja, W. (2018). Investigating privacy implications of biometric voter registration In Kenya's 2017 election Process. Centre for Intellectual Property and Information Technology Law

Mutung'u, G. (2018, June). The Influence Industry Data and Digital Election Campaigning in Kenya. Our Data Ourselves.

National Payment System Regulations (2014).

Office of the Registrar of Political Parties. (2014). A Guide to Political Parties Registration.

Okiya Omtatah Okoiti v. Communication Authority of Kenya & 8 others (2018) eKLR.

Orange Democratic Movement Party v. Independent Electoral and Boundaries Commission (2019) eKLR.

Osborne, H. (2018, March 18). What is Cambridge Analytica? The firm at the centre of Facebook's data breach. The Guardian.

Political Parties Act, n.11. (2011, Kenya).

Prevention of Terrorism Act, n.30. (2012, Kenya).

Proceeds of Crime and Anti-Money Laundering Act, n.51. (2012, Kenya).

Registration of Persons Act, n.12. (2012, Kenya).

Representation of the People Regulations (2001, England and Wales*).*

Rutenberg, I. (2019). Kenya follows the path of European-style data protection. World Privacy Forum.

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154 (3).

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154 (3).

Standing Committee on Access to Information Privacy and Ethics. (House of Commons 2018). Democracy under threat: risks and solutions in the era of disinformation and data monopoly.

Veld, S. (2017). On democracy. *Internet Policy Review*, 4(6).

Vold, K. and Whittlestone, J. (2019). *Privacy, autonomy, and personalised targeting: rethinking how personal data is used.* CGC.

Wanyama, F., Elkit, J., Frederiksen, B. & Kaarsholm, P. (2014). Ethnicity and/or Issues? The 2013 General Elections in Western Kenya. *Journal of African Elections,* 13.