Digital targeting of political messages in Norway

June 2019

Datatilsynet
The Norwegian Data Protection Authority

Contents

SUMMARY 5

INTRODUCTION 6

OUR DIGITAL PUBLIC SPHERE 7

THE TARGETING INDUSTRY 8

THE LEGAL FRAMEWORK 12

MICROTARGETING IN THE US AND EUROPE 15

THE USE OF DATA AND TARGETING TECHNOLOGY BY NORWEGIAN POLITICAL PARTIES 18

What do the parties do? 18

What are the conditions that impact the parties' use of digital targeting technology? 22

Challenges and risk factors 24

CONCLUSION 25

SIX RECOMMENDATIONS FOR THE USE OF MICROTARGETING OF POLITICAL MESSAGES 26

REFERENCES 27

Summary

In this report, we examine the use of digital targeting of political messages. We discuss how digital targeting has been used in political campaigns abroad, and how political parties utilise digital targeting and data analysis in Norway. To survey the use of digital targeting in Norway, we interviewed representatives from all nine political parties currently represented in the Norwegian parliament. In the final part of the report, we offer some practical guidelines for the use of digital targeting in political campaigns.

The targeting of political messaging is generally based on demographic data such as age, gender and place of residence. Microtargeting is a form of digital advertising that is largely based upon information closely associated with the individual person. Microtargeting is based on analyses of among other things the data subjects' behaviour, interests and values, compiled from a number of different sources. The objective is to influence your actions and choices.

Microtargeting of political messages can help voters receive more relevant information, and might also increase political engagement. However, it may have an impact on the privacy of the individual. In addition, it may increase manipulation and discrimination, and also negatively affect the legitimacy of– and trust in – the democratic process.

All the political parties represented in the Norwegian parliament advertise on Facebook. This means that the platform largely sets the premises for the segmentation and advertising tools that the parties end up using. Several parties define their leeway on Facebook as set by the possibilities and restrictions in the platform's ad manager tool. This means that decisions made in Facebook's boardroom have direct consequences for how Norwegian political campaigns are run.

The use of data analysis to increase the efficiency of door-to-door campaigning may, in certain circumstances, enable the targeting of smaller segments, such as residential areas or households. The use of this type of technology varies among the surveyed parties. If analyses purchased from an external agency reveal where persons with a specific voter profile reside, this would in many cases involve the processing of personal data. There is also a risk of re-identification when this kind of technology is linked to data on geographic location on street and household levels. Assumptions based on this data, such as how a certain person may vote, may in some cases constitute personal data.

The uploading of a party's own data (such as membership lists) to Facebook and other advertising platforms in order to customise their own target groups, is currently an ethical line the parties are not willing to cross. However, some parties admit to having previously experimented with this. The way Facebook allow targeting based on finely filtered categories such as interests and behaviour, means that the parties can easily create precise target groups without the use of their own data. In this process, many ethical and legal issues are not necessarily being fully considered.

None of the parties have established written guidelines for the use of personal data and digital microtargeting. This can make the parties vulnerable to slipping into more invasive targeting methods.

Microtargeting requires significant resources. Most parties state that they neither have the resources nor see the value in focusing on very small segments. This means that the segments that are used are often not specific enough to represent a threat to privacy. Resources are also important with respect to which external agencies the parties can use, and which tools they can utilise.

The social, political and economic conditions that presently restrict the parties' use of microtargeting may change. Furthermore, many of the parties use external companies that process data on their behalf. This may contribute to microtargeting becoming more extensive in the future. For example, election campaign budgets may increase and targeting technology may become cheaper and more user-friendly.

The findings in this report correspond with findings from similar studies from other European countries, where it is pointed out that modest budgets, the organisation of the political systems and ethical and legal barriers contribute to the fact that microtargeting is not done to the same extent as have been the case in the US and the UK.[1, 2]

[1] Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. H. (2017). Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. *Internet Policy Review, 6*(4)

[2] Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political microtargeting in Germany. *Internet Policy Review, 6*(4)

Introduction

On the 17th of March 2018, various media outlets published the first articles on what came to be a long line of disclosures on what was then a relatively unknown company called Cambridge Analytica.[3, 4] The company had unlawfully gained access to tens of millions of Facebook profiles, which they analysed and then utilised to run political influence campaigns for Donald Trump's election campaign in the US.

The Cambridge Analytica case led to increased scrutiny on the use and misuse of personal data in the context of election campaigns. For example, the Information Commissioner's Office in the UK have conducted a large scale investigation into the companies involved in the Brexit referendum. Furthermore, in connection to the EU election held this spring, the European Data Protection Board made a statement on the targeting of political messages. In 2019, the Dutch Data Protection Authority initiated an audit to expose how the political parties are compiling and utilising personal data in marketing political messages.[5]

In the autumn of 2019, local government elections will be held in Norway. Even though election campaigns in Norway are increasingly digitalized, little information is available on how digital targeting and data analysis are being utilised for campaigning purposes. With this report, The Norwegian Data Protection Authority hope to generate more knowledge on the use of such methods by the Norwegian political parties.

Targeting of political messages is not illegal, nor is it necessarily problematic. Parties, politicians and pressure groups have targeted specific messages to groups in order to increase their market penetration since the mid-1800s. However, technological developments in the last couple of decades have made it possible to compile and compare more information on voters than ever before, and this is being used to target messages more precisely.

With the help of data analysis and targeting technology, parties can persuade and create advertisements with themes and arguments that influence individual voters, without the voters even knowing or understanding exactly why they are receiving that particular message.

The use of microtargeting for political influencing can have profound consequences on the privacy of the individual – but also for the democratic public sphere. In addition, it may make a political system vulnerable to manipulation, lead to discrimination, and negatively affect the legitimacy of – and trust in – the democratic process.

Elections all over the world are increasingly characterised by the fear of manipulation, "fake news" and interference in the election process by hostile states. These issues are only briefly touched upon in this report. The focus of our report is primarily on the political parties' use of personal data to target political messages in an election campaign.

In connection to the work on this report, we interviewed representatives from all nine political parties currently represented in the Norwegian parliament. We asked them about their use of, and attitudes toward, micro-targeting and data analysis in an election campaign context. The interviews were conducted in March and April of 2019.

In the first part of the report we address microtargeting: what it is, which actors are involved, and how microtargeting has been utilised in elections in the US and Europe. We then review the legal framework that personal data legislation imposes on the use of personal data in digital election campaigns.

In the second part of the report we proceed to present our findings and identify key challenges. Based on these challenges, we conclude by giving practical guidelines for the use of digital targeting in election campaigns.

[3] Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, 17 March). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[4] Cadwalladr, C., & Graham-Harrison, E. (2018, 17 March). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[5] Autoriteit Persoonsgegevens. (2019, 15 February). Verkennend onderzoek naar gebruik persoonsgegevens in verkiezingscampagnes. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennend-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes

Our digital public sphere

In 2019, we can no longer refer to the concept of the public sphere without acknowledging the fact that a great deal of our common political discourse has moved into the digital realm. The public sphere, the term that describes the sphere in which citizens meet and where rational arguments are put forward – regardless of status and identity – is a central component of every democratic society. The ideal of the public sphere, first formulated by the German sociologist Jürgen Habermas in 1962, presumes that meeting spaces – spheres – where citizens participate in a free exchange of opinions, are free and open to all.

Throughout the years, various public spheres have had differing qualities and technological characteristics, and these have had tremendous influence on the nature of public discourse. Smoke-filled cafés in the 1700s, large public meetings and the columns of local newspapers are all typical public spheres with unique qualities that have both restricted and afforded specific forms of public discourse.

Changes that have influenced the public spheres in Norway include the breakthrough of television media, and that the printed press has moved from being loyal to a particular party or political movement, to becoming independent of party politics. The greatest change in the last decade has been the emergence of social media as a prolific arena for public discussion, debate and political activity. In short, the public sphere, as is the case for many other social spheres, has become digitalised.

Consequently, a major challenge has arisen in that regulations imposed by the parliament on traditional public spheres do not apply in the new digital arenas. In Norway, as in many other countries, the broadcasting of political advertising on television is not permitted. However, political messages are still lawfully communicated with sound and images on social media.

The world's democracies are in a situation where an important part of our political arena increasingly exist on platforms that do not have the same clearly defined societal roles as those held by traditional media. Digital platforms also have major economic incentives to resist democratic control.[6]

For digital platforms, economic growth is largely generated by advertising revenue. Political messages have thus become attractive sales commodities on the profitable advertising market.

A well-functioning *public* sphere is also dependent on citizens having a *private* sphere that is shielded from the public spotlight. The fact that today's public sphere is increasingly being moved over to the digital arena means that opinions and activities are monitored, registered, and stored, functioning as databases for commercial enterprises.

The huge growth in computer processing power, decreasing costs for data storage and the development of sophisticated, complex data analyses models have led to the growth of a profitable industry that targets digital advertising to individuals, based on browsing history, purchasing history, location data, and a wide range of other factors. In recent decades, these methods have increasingly been utilised by political parties to win elections – and this affects our common, democratic public sphere.

[6] Bodó, B., Helberger, N., & de Vreese, C. H. (2017). Political microtargeting: a Manchurian candidate or just a dark horse? *Internet Policy Review*, 6(4).

The Targeting Industry

The targeting of political messages is not a new phenomenon. A local politician can run his or her election campaign at a local train station based on the assumption that those using the station have a particular interest in quality public transportation. The targeting of political messages is often based on demographic data such as age, gender and place of residence. The amount of information collected by major digital platforms has created greater accuracy and precision in the analysis of the electorate.

In contrast to traditional targeting, microtargeting is based on information that is closely associated with you as an individual, such as your interests, values, habits and behaviour.

Based on this information, advertisements can be created with themes and arguments specifically tailored to groups or individuals. In a political campaign, microtargeting can also be used to identify neighbourhoods and households with a large proportion of persons that potentially can be persuaded to vote for a specific party.

Microtargeting technology offers political parties the opportunity to move from focusing on large target groups to providing more specific messages at the individual level.[7]

Digital advertising gold

The digital advertising industry is comprised of analysis agencies, PR firms and advertising and consultancy companies that over decades have perfected the art of analysing data from surveys, focus groups and voter statistics. This has been done to ensure that the sale of products and political messages is done as effectively as possible.[8] The rise of the Internet and social media has given this industry even more powerful tools in its search for comprehensive databases that provide the best analyses and the greatest potential for profit.

Microtargeting

Microtargeting is a type of targeted digital advertising that analyses personal data collected from several different sources, with the goal of influencing a person's actions.

The information can be obtained from a broad range of sources, including Internet and social media activity through the use of cookies and tracking images (web beacons/pixels).

Microtargeting is a fundamental part of the digital advertising industry, and has turned Google and Facebook into some of the world's most valuable companies. Beyond the use of targeted personalised advertising in the commercial sector, political parties and candidates have the past ten years increasingly benefited from the same methods.

Social media also functions as a communication- and influencing channel that even smaller operators can effectively use.[9] Most of the digital tools used in political campaigns have been developed, tested, refined and perfected by companies within the digital advertising industry.[10]

The digital advertising industry uses sophisticated data analyses on huge sets of data to design advertisements tailored specifically to you. In a political context, the same methods can be used to mobilise, engage and influence voters to support (or resist) a political candidate, party, or policy. Data analyses can even include models that predict a person's psychological traits (also known as psychometrics).[11] For example, a person that the model assumes is outgoing and open to new experiences and ideas may receive a different message than a person assumed to be an introvert, who

[7] Bartlett, J., Smith, J., & Acton, R. (2018). *The Future of Political Campaigning*. Demos. Retrieved from www.demos.co.uk

[8] Chester, J., & Montgomery, Kathryn, C. (2017). The role of digital marketing in political campaigns. *Internet Policy Review, 6*(4)

[9] Gibson, R. K., & McAllister, I. (2015). Normalising or Equalising Party Competition? Assessing the Impact of the Web on Election Campaigning. *Political Studies, 63*(3), pp. 529-547

[10] Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday, 19(7).*

[11] Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behaviour. *Proceedings of the National Academy of Sciences, 110*(15), ss. 5802-5805. doi: https://doi.org/10.1073/pnas.1218772110

may be more comfortable with routines and familiar experiences.

Political microtargeting happens in different ways; however, the methods depend on the infrastructure developed by the digital advertising industry. This industry, and the challenges they represent to privacy, was thoroughly analysed in our report «Det store datakappløpet» ("The Great Data Race").[12]

The digital advertisement industry is dominated by two major actors, Facebook and Google. These companies generate enormous revenue from tailoring digital advertisements to individuals. Facebook's advertisements are generally created using their own advertisement tools, whilst Google's most profitable advertising system is based on automated real-time auctions between advertisers who pay to have their advertisements placed on relevant websites.

Companies specialising in political influence

In recent years, a number of companies have emerged that specialise in political targeting. Cambridge Analytica was such a company, and its parent company, SCL Group, openly boasted of its role in more than 100 democratic processes in over 30 different countries.[13]

NationBuilder has from its start-up in 2008 offered politicians, parties and activists comprehensive software for grassroots organising, fundraising and voter communication, largely based on the data analysis of available personal data. The company has been used by American politicians for a number of years, and has also played a prominent role in European elections, such as the French presidential election in 2017.[14]

Other major political software services include Fundly, Ecanvasser and TrailBlazer. Even though these services specialise in different areas, their common denominator is that they offer software designed for political campaigning and that they are dependent on a large amount of personal data in order to provide a competitive product.

Political microtargeting puts pressure on personal data protection, increases vulnerability to manipulation, and can damage trust in the democratic process.

However, there are also clearly positive repercussions that should not be underestimated. Access to specific segments, combined with relatively cost-effective communication channels, can potentially be decisive for smaller parties and organisations struggling to break into the editor-controlled media and in the public sphere. In addition, tailored information can increase engagement and voter participation among groups that otherwise would not have had a particular interest in politics or voted in elections.

Facebook is making changes

Several American technology companies, particularly Facebook, have been placed under political pressure in the wake of the Cambridge Analytica scandal. Some companies have responded by gradually introducing changes and restrictions on how advertisers can utilise their tools, with particular focus on advanced filtering functions for finding and defining target groups.

Facebook has implemented several changes in the last year:[15]

- The function "Partner Categories" has been removed. This function made it possible for advertisers to compare personal data that they themselves had collected, with information offered by data agencies such as Acxiom and Datalogix. This third-party information was often extremely comprehensive, and included demographics, interests, behaviour, values, purchase history and a number of other variables.

- Advertisers that construct their own target groups based on e-mail addresses and telephone numbers that they themselves have compiled, must have permission from the persons from whom they have collected

[12] The Norwegian Data Protection Authority. (2015). *Det store datakappløpet: Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet.*

[13] Ghoshal, D. (2018, 28 March). Mapped: The breathtaking global reach of Cambridge Analytica's parent company. *Quartz*. Retrieved from https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/

[14] O'Brian, C. (2017, 14 July). How NationBuilder's platform steered Macron's En Marche, Trump, and Brexit campaigns to victory. *Venturebeat*. Retrieved from https://venturebeat.com/2017/07/14/how-nationbuilder-helped-emmanuel-macron-secure-a-landslide-in-frances-legislative-elections/

[15] Goldman, R. (2018, 21 December). *Changes We Made to Ads in 2018*. Retrieved 30/4/2019 from Facebook Business: https://www.facebook.com/business/news/changes-we-made-to-ads-in-2018

information. However, the fact that this verification function has been handed over to the advertisers implies that Facebook have transferred the responsibility of ensuring the lawful processing of information onto the advertisers.[16]

- An advertising banner has been set up that makes it possible to gain access to information about all advertisements being run at any given time on a specific page. In addition, the platform has established a public, searchable archive for political advertisements, with a planned storage period of seven years.

- Restrictions in Facebook's advertising solutions disallow a political party (or any other actor) to target an advertisement to less than 1 000 persons.

- In certain countries, Facebook have also introduced a verification function for advertisers that offer election-related content. This requires proof that the user is an actual political actor in the relevant country, and that the sender of the advertisement is clearly displayed. This function has been introduced primarily to reduce the spread of so-called “fake news” and is a response to the scandals surrounding Russia's interference in the American election campaign in 2016. At present, these changes have only been implemented in Brazil, India and the United Kingdom, as well as the US.[17]

Despite these changes, there remain major legal and ethical challenges associated with the technology companies’ use of personal data in their analysis tools. For example, it is possible for users of the advertising tools to circumvent many of the restrictions implemented by Facebook.[18] Independent companies that have developed software that tracks the extent of political advertising on Facebook, have been excluded from the platform.[19] The software also revealed that Facebook's own system for identifying political advertising did not flag advertising from the American lobby group National Rifle Association, an organisation that in 2016 spent $100 million on lobbying American politicians.[20]

[16] Constine, J. (2018, May). Facebook demands advertisers have consent for email/phone targeting. *Techcrunch.* Retrieved from https://techcrunch.com/2018/06/13/facebook-custom-audiences-consent/

[17] Schiff, S. C. (2018, 6 December). Increasing Ad Transparency Ahead of India’s General Elections. *Facebook Newsroom.* Retrieved 30/4/2019 from https://newsroom.fb.com/news/2018/12/ad-transparency-in-india/#

[18] Faizullabhoy, I., & Korolova, A. (2018). *Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions*

[19] Waterson, J. (2019, 27 January). Facebook restricts campaigners’ ability to check ads for political transparency. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2019/jan/27/facebook-restricts-campaigners-ability-to-check-ads-for-political-transparency

[20]Merrill, J. B., & Tobin, A. (2019, 28 January). Facebook Moves to Block Ad Transparency Tools — Including Ours. *ProPublica.* Retrieved from https://www.propublica.org/article/facebook-blocks-ad-transparency-tools

Tracking Internet activity

Many erroneously believe that the services we use on the Internet are free. In reality, companies earn money from the personal data that is collected every single time we open a web page, click on a link or comment on a Facebook status. This enormous harvesting of data is explained, and often defended, by claiming that it is in the users' interests for the companies to be able to offer personalised and relevant content. For example, if you click on many property advertisements, more such advertisements will appear on the web pages you visit. Friends that you connect with on social media will appear more often in your feed than those you seldom have contact with.

Your online behaviour is tracked in many ways and most of these ways are hidden from you. When a property advertisement follows you around on the Internet, it is often because you are being tracked by one or more cookies. Cookies are small files that are installed on your computer when you visit a web page. They make it possible to recognise you over time and thereby store information about your behaviour online.

Normally, a distinction is made between first party and third party cookies. First party cookies are installed by the website owner and are normally used to analyse Internet traffic. Third party cookies, however, are operated by companies in the advertising industry. These companies can have cookies placed on countless numbers of web pages, meaning they can build detailed profiles on each individual Internet user.

This tracking technique has become even more advanced in recent years. Whereas previously, the stream of information was limited to the computer you used, companies can now track you across all devices connected to the Internet, and compile this information to build one single user profile. This development is described as a shift from device tracking to personal tracking.

Google, Facebook and the other technology companies use the information collected on everyone using their services to sell advertising space to the highest bidder in digital advertising markets. Advertisement auctions are conducted automatically in real time. This means that when you open a web page, information about you is sent to an external server operated by companies that have installed tracking cookies on that web page. Your profile is analysed, and a tailored advertisement is then shown on the web page you opened. This process takes approximately 200 milliseconds, and can be combined with so-called A/B testing that continuously provides feedback about the effectiveness of the advertisements, which in turn can be used to make further adjustments.

The legal framework

All companies that process your personal data must have a lawful basis for the processing. This also applies to political parties, whether they process your personal data in relation to your party membership, or whether they use your personal data to market their party directly to you.

§ Special categories of personal data

Information concerning a person's political opinions is defined as a *special category of personal data,* previously known as "sensitive personal data".

Since your political opinion is information you may not want to disclose to others, or information you may feel uncomfortable not having control over, this information is subject to special protections under the General Data Protection Regulation (GDPR), Article 9 no. 1.

The basic principle is that it is unlawful for companies to process personal data relating to political opinions. However, it is lawful if the company can demonstrate a lawful basis of processing according to article 6 no. 1, and prove that the processing complies with at least one of the exception conditions in article 9 no. 2, for example that you have first given valid consent.

We can use an example: A political party publish an image of you on their Facebook page. In the image, you stand smiling in front of their campaign stand, which is covered in large party logos, and the text below the image states "Today we recruited many new members to the party!" Since this picture could indicate something about your political opinions, the political party would have to account for a lawful basis of processing in accordance with article 6 no. 1, as well as demonstrate that one of the conditions of exception has been met. If this is not the case, it will not be lawful for them to publish your image. In this case, valid consent would be the most suitable lawful basis of processing and condition of exception.

In addition, if you have given your consent that the image may also be used for marketing purposes, then a more difficult issue could arise. Let us imagine the following scenario: Peder is looking through his news feed on Facebook, and sees an advertisement with the image and text: "We want these matters to be given priority in Lillevik. Join our campaign!" Peder has never contacted, interacted with, or engaged with the party or its posts on the Internet. How has this advertisement become part of Peder's particular news feed? Part of the election campaign strategy of the party in question is to utilise targeted advertising in social media in order to reach out to more voters. The party sends out political advertisements on social media to men aged between 20 and 40 who reside in Lillevik. The party has selected these criteria because statistics from previous elections indicate that persons in this category, such as Peder, represent a core voter group for the party.

Derived data is also personal data

The big question is then: Is the political party processing personal data concerning Peder's political opinions when he is the recipient of this type of targeted marketing? If this is the case, they are processing a special category of personal data that is only lawful if one of the exception terms is met, such as the data subject's unambiguous, freely given, specific and fully informed consent.

Those that use targeted advertising often apply assumptions, not factual knowledge. If you see an advertisement for a vacuum cleaner, this may be because someone believes that you are *likely* to purchase a new vacuum cleaner – not because they know this for certain. Such assumptions are often based on other information they hold about you, along with statistical correlations. For example, it may be that a social media is aware that you recently moved, and that those who have moved are statistically more likely to purchase a vacuum cleaner for a period of time. Such assumptions about who we presumably are and what we presumably will do is called *derived data* – data that is generated on the background of other data. The GDPR applies to both factual information and derived data.

In Peder's case, the targeting criteria are very general, combined with the fact that the party has not made any assumptions about how certain persons will vote. Instead, they have sent the message to a random group of people within a *very broadly defined* segment where the number of potential voters are expected to be higher than in the general population. The combination of a very simple, general statistical context with the absence of a personal focus, means that the party does not process personal data concerning Peder's political opinions in this example.

If one of these two premises changes, this may instead become processing of personal data on political opinions:

- If the party or social media has carried out finer filtering and analysis to create segments that indicate a person’s political opinions with a certain accuracy (based on a combination of demographics, geography, profile information, web pages followed and friend lists, for example), this data is no longer simple and general statistics. At that point, it has clearly turned into political profiling and thus the processing of special categories of personal data on individuals placed in this segment.

- The same applies if the focus is on how Peder is likely to vote – even if the assumption is based on very simple data. The same also applies if the focus is on the person or persons who live in the household at 2 Lillevik Road, in contrast to those in the household at 3 Lillevik Road. That “Peder is likely to agree with our party on many issues” is an item of personal data, based on its purpose, content and effect.

The line between the two cases can be somewhat vague; however, the point is that little is required before it becomes a matter of personal data concerning political opinions, even though it involves simple assumptions and derived data.

The same will apply to parties who use door-to-door canvassing as a method of reaching out to existing and potential voters. If a party knocks on Peder's door because, through experience and analysis of previous election results, they know that it is a reasonable area in which to go door-to-door, they will not process data on Peder’s political opinions. Just as in the example above, they will not process data on Peder's political opinions if they knock on the doors of men aged between 20 and 40 in Lillevik. However, if the party had knocked on Peder’s door based on a more intricate and finely filtered analysis, where several elements combined inform the party that Peder is likely to be interested in their message, they will then be processing data concerning his political opinions.

One of the exceptions is that it is lawful to process special categories of personal data if the processing relates to personal data which are manifestly made public by the data subject. It is easy to think that this could be the case when the data subject, on his/her own Facebook profile has published their interests and other personal data, which can be used to make an assumption about the person’s political opinions. However, this exception must be interpreted narrowly, and the European Data Protection Board (EDPB), in Statement 2/2019 of 13 March 2019, has stipulated that this exception cannot be used to legitimise processing of this type of derived data.

The parties are responsible

When political parties decide on the purpose of processing personal data, and the tools to be used, they are then characterised as a *data controller*. According to the GDPR, the data controller is the primary entity principally responsible for complying with the regulation. This is anchored in the accountability principle (article 5 no. 2).

This stipulates that the data controller must: process your personal data in a lawful, fair and transparent manner; have a lawful basis of processing for each instance of processing carried out; must handle personal data in a secure manner; ensure that you as the data subject can assert your rights – and many other obligations. The requirement for transparency means, among other things, that the data controller must provide you with concise and understandable information about how your data has been obtained and what it will be used for. They carry this responsibility whether they process information about you in relation to your membership in a political party, or whether they choose to use platforms such as Facebook to reach out to existing and potential voters.

Profiling and automated decision-making

Profiling means to evaluate, analyse or predict personal aspects of a person. If a political party or a company uses your personal data to predict your personal preferences concerning your political opinions, they are, in such a case, profiling you. This type of profiling involves a distinct risk to both privacy and free formation of opinion, as it concerns a simplification of reality and categorisation of persons. This type of categorisation can vary in terms of accuracy, and can lead to filter bubbles and polarisation. In cases where processing of data concerning political opinions is permitted, it is therefore important that measures are in place to ensure that the processing is fair.

According to the GDPR, as a data subject, you in principle have the right to *not be subjected* to a decision based solely on *automated processing,* including profiling, which produces legal affects you or *similarly significantly affects* you (article 22 no. 1).

The question is, therefore, whether targeting of political advertisements specifically to you involves a decision that *significantly affects* you. This is not a question that can be answered simply, and the answer is likely to depend on the specific situation.

Still, the European Data Protection Board has stated that fully automated targeting of political messages, in certain circumstances, "similarly significantly", will affect the data subject. If this is the case, this is only lawful after valid consent has been collected.

Microtargeting in the US and Europe

Microtargeting of political messages is currently most widespread in the US. This is due to a number of factors, such as weak privacy legislation, liberal regulations concerning election campaign financing, a strong position on the freedom of speech, how the election system is organised, and a data agency industry that offers the most advanced analysis tools to be found.[21]

However, microtargeting has also been utilised to varying degrees by European political parties in a number of countries. In this chapter we will therefore look more closely at how microtargeting has been used in political campaigns in the United States, the United Kingdom, Netherlands, Germany and France.

USA

The Cambridge Analytica scandal sharply brought into focus the use personal data by political actors in modern election campaigns. However, Cambridge Analytica's methods did not differ sharply from previous practice; it was rather a furtherance of relatively common methods used in the modern political influencing industry.[22, 23] Barack Obama is considered to be the first presidential candidate to carry out an extensive, data driven election campaign. Both when he was elected in 2008 and re-elected in 2012, sophisticated analyses of personal data, combined with extensive door-to-door campaigning, were a central part of the election campaign that led to a relatively unknown senator becoming the 44th president of the United States.

However, the Trump campaign benefited from break-throughs in the development of microtargeting technology, such as the ability to track activity across devices[24], and the gradual increase in voter datasets. It has emerged that Cambridge Analytica, on behalf of the Trump campaign, unlawfully harvested approximately 87 million Facebook profiles and combined this information with a wide range of other databases. The model developed by the company included, according to their own statements, between 3,000 and 5,000 data points for each person. In addition, they employed a psychological personality test that measures personality traits according to five variables (the five-factor model, also known as "The Big Five"). Persons who were seen as likely swing voters in the important swing states were further bombarded with tailored political messages, delivered exclusively to smaller groups with the help of so-called "dark posts", meaning that the advertisements shown in a person's news feed were hidden to other users.

The Trump campaign also targeted voters that were unlikely to vote for Trump, but that the model predicted could be influenced to abstain from voting. These were mainly voter groups that predominantly voted for the Democratic Party.[25]

This disclosure was the direct reason as to why Facebook CEO Mark Zuckerberg was called to testify before Congress. The incident is one of many Facebook scandals of the last couple of years, and is continually referenced in discussions on the power of social media in modern society. In addition, the disclosures were seen in context with broader socio-political trends, such as increased polarisation, the spread of "fake news" and the interference of foreign countries in democratic elections.

United Kingdom

In the wake of the EU referendum in the United Kingdom, it was revealed that the official campaigns on both sides of the Brexit debate utilised the same

[21] Bennett, C. J. (2016). Voter databases, microtargeting , and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law, 6*(4), pp. 261-275

[22] Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R., & Wright, G. (2019). *Personal Data: Political Persuasion. Inside the Influence Industry. How it Works*. Tactical Tech. Retrieved from https://tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf

[23] Hersh, E. D. (2015). *Hacking the electorate. How campaigns perceive voters*. Cambridge University Press.

[24] Lotame.com (2017, 4. oktober). The Benefits of Cross-Device Marketing, retrieved 2/5/2019 from https://www.lotame.com/benefits-cross-device-marketing/

[25] Solon, O. (2018, 16 May). Cambridge Analytica whistleblower says Bannon wanted to suppress voters. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony

influencing methods as those used in the Trump election campaign. Cambridge Analytica played a major role also here. It is estimated that the official campaign for Britain to leave the EU, in the days before the referendum, sent out targeted political "dark advertisements" that achieved approximately 1 billion page views.[26] Cambridge Analytica's role in the single most important democratic process in modern British history remains the subject of intense criticism and investigation.

The United Kingdom's Information Commissioner's Office (ICO) reviewed how political parties used data in relation to the national parliamentary election in 2017. It was revealed that a company that offered advice to expectant mothers and parents of small children had sold data about one million of its users to a data agency. This data was subsequently used by the Labour Party to tailor political advertisements to new mothers before the election in 2017.[27] In addition, microtargeting in digital media played a major role when the Conservative party won the parliamentary elections in 2015.[28]

In 2018, the ICO inspected 170 actors involved in elections in the United Kingdom. This was the most extensive audit ever to be carried out by a data supervising authority. After an 18-month investigation, a number of companies, including Facebook, were fined for breaches of privacy legislation.[29]

The election system in The United Kingdom is, similar to the American one, essentially a two-party system. In addition, political parties in the country have access to a wide range of national registers and databases that parties in other parts of Europe do not.[30] Therefore, some of the opportunities for the extensive use and misuse of political microtargeting are more easily available to United Kingdom parties and politicians than in other European countries, including Norway.

Netherlands

The Dutch parliamentary elections in 2017 are one of few elections that have been subjected to academic

Norwegian microtargeting

There have been several cases in Norway in which political parties have been criticised for using invasive targeting technology in election campaigns.

The Conservative party sent out an email to its members four days before the election in 2013. According to the Norwegian Broadcasting Corporation those that clicked "yes" to taking part in a campaign promotion on Facebook were directed to Facebook, where they accepted terms and conditions, including that their friends lists would be passed on to the analytics company Bisnode Analytics. The company received access to names, dates of birth and residences from friends lists, and built a dataset that contained information as to how likely it was that the person would vote for the Conservative party. A list of the 25 most likely Conservative party voters was sent back to the users, who were encouraged to send them a personal message about the election. None of the friends of those that downloaded the application were informed that they were allocated a score by Bisnode Analytics. This concerned approximately 10,000 persons.

The day before the election in 2017, the Labour Party sent out text messages to half a million voters. The Labour Party had purchased access to the telephone numbers from IPER Konsumet, a company that offers address databases. The company compiled the data and sent out text messages encouraging recipients to vote for the Labour Party. The selection was based on demographics and geography at a regional level. Despite the fact that this did not breach any personal data privacy laws, it drew a great deal of criticism.

[26] Cadwalladr, C. (2017, 25 November). Vote Leave donations: the dark ads, the mystery 'letter' – and Brexit's online guru. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2017/nov/25/vote-leave-dominic-cummings-online-guru-mystery-letter-dark-ads

[27] Kelion, L. (2018, 11 July). Emma's Diary faces fine for selling new mums' data to Labour. *BBC News*. Retrieved from https://www.bbc.com/news/technology-44794635

[28] Ross, T. (2015, 16 May). Secrets of the Tories' «war room». *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/politics/11609570/Secrets-of-the-Tories-election-war-room.html

[29] Nes, C. (2019, 24 January). Høstens valgkamp blir trolig den mest teknologisk avanserte noensinne. *Dagens Næringsliv*. Retrieved from https://www.dn.no/politikk/personvern/malrettet-annonsering/datatilsynet/teknospaltist-hostens-valgkamp-blir-trolig-den-mest-teknologisk-avanserte-noensinne/2-1-526848

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

examination of political microtargeting in continental Europe. A research report from the University of Amsterdam showed how microtargeting was used by Dutch parties, but that the methods used differed significantly from those revealed in the United States and the United Kingdom.[31] The authors highlighted a number of structural factors that influenced the use of microtargeting technology in the Netherlands, such as resources, how the election system is organised, legal restrictions and ethical concerns. In light of the major international attention on this issue, the Dutch Data Protection Authority has initiated an investigation to examine how the parties' service providers use personal data in an election context.

Germany

In Germany, similar restrictions have been found regarding the use of microtargeting by political parties.[32] In line with the findings from the Netherlands, researchers have highlighted several factors that limit the use of microtargeting technology in Germany. These factors include the organisation of the German election system, relatively modest budgets and ethical and legal restrictions. However, in the wake of the parliamentary election in 2017, criticism was aimed at the Christian Democratic Party, CDU, and the centre-right party, FTP, both of whom in 2017 purchased personal data from the German postal service.[33] The data they purchased indicated the political leanings of the residents in specific buildings, and contained personal data such as income, education, and whether the relevant persons owned a car. Still, much of the public debate in the wake of Germany's parliamentary elections in 2017 has dealt with the influence of foreign actors and voter manipulation.

France

Methodical and precise targeting was a central component of the French presidential elections in 2017.[34] Prior to the elections, the French Data Protection Authority (CNIL) provided guidelines aimed at political parties, regarding the use of data compiled from social media.[35] A large number of candidates utilised various digital campaigning tools, such as the American platform NationBuilder, for voter profiling.

CNIL was also involved in several other cases. For example, they intervened in a case from 2016, in which the campaign of Nicolas Sarkozy utilised an application for door-to-door campaigning, in which data obtained from social media was coupled with geolocation.[36] However, it was the hacker attack on Emmanuel Macron's campaign organisation in the hours before the election that gained the most attention. This resulted in the leaking of tens of thousands of emails and documents from Macron's campaign organisation. [37]

EU

The European Data Protection Board have also been concerned about the consequences of microtargeting on European democracies. Because of this, the Board has issued a statement aimed at political parties that process personal data as part of their political campaigns.[38] Among other things, the Board emphasised that personal data compiled from social media cannot be processed without complying with requirements for openness, specification of purpose and lawfulness.

[31] Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. H. (2017). Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. *Internet Policy Review, 6*(4).

[32] Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political microtargeting in Germany. *Internet Policy Review, 6*(4

[33] Chase, J. (2018, 1 March). Deutsche Post sold voter microtargeting data to CDU and FDP. *Deutsche Welle*. Retrieved from https://www.dw.com/en/deutsche-post-sold-voter-microtargeting-data-to-cdu-and-fdp/a-43218488

[34] Duportail, J. (2018). The 2017 Presidential Election: The arrival of targeted political speech in French politics. https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-france.pdf

[35] Commission Nationale de l'Informatique et des Libertés. (2016, 8 November). *Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?* Retrieved 7/5/2019 from https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

[36] Le Monde. (2016, 17 November). https://www.lemonde.fr/politique/article/2016/11/17/la-cnil-enquete-sur-knockin-l-application-des-militants-sarkozystes_5032818_823448.html

[37] Willsher, K., & Henley, J. (2017, 6 May). Emmanuel Macron's campaign hacked on eve of French election. *The Guardian*. Retrieved from https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election

[38] European Data Protection Board. (2019). *Statement 2/2019 on the use of personal data in the course of political campaigns.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

The use of data and targeting technology by Norwegian political parties

We have interviewed representatives from the nine political parties represented in the Norwegian parliament. The purpose of the interviews has been to acquire an overview of how Norwegian parties use data and data analysis, along with various digital platforms for microtargeting of political messages. The interviews were conducted in March and April of 2019.

In the interviews, we used the Norwegian Data Protection Authority's ombudsman role to gather knowledge that is of interest to the general public. The findings will also inform the ongoing discussion concerning targeting of political advertising in Norway. We have not carried out audits or looked for breaches of privacy legislation. The parties have shared information voluntarily.

The interviewees are associated with the central party national organisations located in Oslo. Consequently, the report provides an overview of overarching strategies and tools managed by them. We did not review any strategies or tools used by local party offices.

The interviews covered the following themes:

- Which technological solutions and digital platforms do the parties use?
- What data and which data registers are used, and how?
- Which and what type of partners do the parties cooperate with?
- What attitudes do the parties have regarding the use of targeted marketing of political messages?

What do the parties do?

Social media

Facebook is the dominant digital platform for political messaging in Norwegian elections. All the parties informed us that they used Facebook's advertising tools, and several added that the parties' financial resources for advertising have gradually moved away from newspapers and towards digital platforms.

By using Facebook's advertising tools, the parties are able to select target groups that will receive a political advertisement. Facebook permit targeted advertising based on a range of data that can easily be accessed by the parties. In the interviews, it became evident that the political parties in Norway create target groups on Facebook based on data relating to geography (location), demographics (such as age and gender), interests and behaviour. Facebook also permit exclusion of target groups, where a specified group can be excluded from seeing the ad. None of the parties said that they used this functionality.

Restrictions in Facebook's advertising solutions prevent advertisers from targeting an advertisement to fewer than 1,000 persons. This led to one party experiencing challenges of running targeted advertising aimed at voters in rural districts, where target groups are often comprised of fewer than this threshold number. The same party also stated that Facebook's advertising solution is therefore more suitable to targeting voter groups residing in towns and cities.

Beyond Facebook's general advertising solution, Facebook offer two other functions to help further improve targeting. These are **"Custom Audiences"** and **"Lookalike Audiences"** – (see fact box on the following page). With these functions, it is possible to utilise additional data sources to create target groups for political advertising.

Eight of the nine parties stated that they had used one or both of these advertising solutions. For example, one party used Lookalike Audiences to target advertisements to persons that had a profile that was similar to persons that followed the party on Facebook.

With the Custom Audiences function, it is possible to target selected persons by uploading personal data that the parties themselves have compiled, and to combine these with information held by Facebook. This can include information about party members' email addresses, telephone numbers and other contact information.

None of the parties stated that they currently upload information they compile from their members for use in Facebook.

One party explained this stance by stating that “they wanted to stay on the right side of what was acceptable”; another party stated that “they made sure that member data was not used for anything else other than what it was intended for”. In the interviews, there was prevailing scepticism toward uploading the parties’ own data into Facebook’s advertising solutions. It appears that using members’ personal data for advertising on Facebook is an ethical line that none of the political parties are willing to cross. **However, even though the parties state that they do not do this at present, some of the parties have done so previously.**

While most of the parties advertised exclusively on Facebook, a few of them also used Instagram. During the interviews, YouTube and Twitter were also mentioned; however, this was chiefly in the context of the parties’ general communication work, not paid political advertising. The use of Snapchat, the image sharing service, has also been discussed; however, in general it has not been assigned the same importance as other platforms. The Conservative party used Snapchat in the 2017 elections, where users could get their own “Erna glasses” or add a filter with the title “Team Erna” – referring to current Norwegian Prime Minister Erna Solberg.

Data analysis for targeted door-to-door canvassing

Data analysis is increasingly being used to increase the effectiveness of door-to-door campaigns. There are several companies that offer various forms of data analyses that identify locations that offer the greatest chance of success during door-to-door canvassing. They often do this by highlighting constituencies, neighbourhoods or households that are appropriate to visit.

Seven of the political parties we interviewed stated that they would be carrying out door-to-door canvassing in the coming election campaign. Of the seven parties, four responded that they used data analysis to target the areas they would campaign door-to-door. Two of the parties that did not use data analysis to target door-to-door campaigns said that they selected areas for house calls based on local knowledge or intuition.

Parties that carried out or received data analyses in advance of door-to-door campaigns often use information concerning previous party affiliation within the constituency, the type of dwelling and the proportion of gender and age in a specified area. Several of the parties use digital systems where campaigners and volunteers register how the visit have gone. One party

How do Facebook's segmenting tools work?

1. **Custom Audiences**
   Custom Audiences is a targeting function in Facebook’s advertising portal that allows you to “reconnect with the people who have already shown interest” in your organisation. This means that advertisers can use information obtained from Facebook accounts controlled by the advertisers, or other platforms than Facebook's own, in order to target advertisements.

   Custom Audiences can be constructed in several different ways, such as:

   - By the advertiser uploading its own customer lists/datasets, that Facebook connects with user profiles. Customer lists will typically contain email addresses or telephone numbers.
   - By using information obtained from the advertiser’s home page, through a Facebook pixel (a tracking image). Advertisers can define which criteria (actions) that will apply, so that the visitor of the home page is included in the target group being set up. Such criteria can include pages of the website that have been visited by the user, or the length of time spent by the user on each page. Advertisers can include and exclude pages according to their own requirements.
   - By using information about interactions on Facebook's platforms. For example, this will show who has viewed or liked posts on a specific Facebook or Instagram page controlled by the company.

2. **Lookalike Audiences**
   Lookalike Audiences is a function that offers advertisers the opportunity to target advertisements to a customer group that share characteristics with those who already have expressed interest in the company or organisation. The tool uses data relating to demographics, interests, social network and users’ activity in news feeds, and offers advertisers a “lookalike” of its existing customer base.

stated that they had previously done this on paper; however, this had now been digitised.

The technology used for increasing the effectiveness of door-to-door campaigning divides the population into target groups and is often interfaced with mapping solutions. In some of the tools, campaign volunteers can create a pre-defined route to enable them to only make calls in areas with a high proportion of the desired target group. For example, a party that is popular among female voters with a high level of education in a specific constituency, can direct its resources towards areas with a significant proportion within this target group.

Several of the tools used by the Norwegian parties contain an integrated feedback function; however, the party stated that the information registered in the function is very limited. The registered data primarily deals with the experience of campaigners and what it was like going door-to-door. This feedback is not tied to households, but to constituencies or areas. Exactly what is said during a door-to-door call, or information concerning political views, is not registered. An important reason for incorporating this type of feedback system was that it was said to be motivating for the election campaign volunteers.

Coupling databases containing personal data to interactive mapping services can be problematic from a privacy viewpoint. If mapping solutions make it possible to go all the way down to the household level, the information will be considered to be personal (information pertaining to the person or persons living in the specific residence).

In the same way, feedback systems based on door-to-door campaigns can put pressure on privacy, as these facilitate registration of more detailed information.

Programmatic advertising

Approximately half of the parties in the Norwegian parliament use political programmatic advertising. Some of them use advertising agencies to run these campaigns.

Parties that utilise programmatic advertising target their advertising based on geography, age, gender, education and occupation. In several of the interviews, it emerged that the programmatic advertising used is based on data concerning search words, network, geography, gender, age and IP addresses. None of the parties stated that they used personal interests or other person-specific preferences as criteria for advertising.

Knock knock

There are several tools that can be used to profile households.

The Mosaic service classifies the population in Norway into “lifestyle types” and is used, among other things, in analysis of geographical areas and households. The data applied as a basis for Mosaic is based on information about demographics, finance, registered cars, urbanism and dwelling. In Norway, the marketing agency InsightOne owns the rights to Mosaic.

The Irish company Ecanvasser offers a location-based door-to-door canvassing application, where campaigners can plan a route and coordinate visits. Ecanvasser can also be synchronised with NationBuilder, a platform that, among other things, can be used to mobilise volunteer election campaign workers.

Representatives from two parties commented that, in many instances, they felt that providers had “pressured them” to use their services. Most of our sources stated, however, that they did not regard the provider industry as being aggressive. Two of the parties also questioned the effectiveness of programmatic advertising. One of the representatives stated that programmatic advertising gave poorer results than advertising on Facebook or Instagram. In one interview, it was also stated that it gave little value for the money spent.

Data compiled from party web pages

For the most part, the political parties gain access to datasets concerning voters from external agencies. Additionally, the parties hold data concerning activity on their own web pages. In the interviews, it emerged that most of the parties utilise various methods to track or analyse the behaviour of visitors to their own websites.

In addition to interviewing representatives from the political parties concerning the type of data collected from their web pages, we examined the parties’ use of cookies. We used the software “Awesome Cookie Manager”, which displays cookies along with their properties. Using this application, we were able to identify content on the parties’ websites (see table below).

Content on the parties' websites.	Proportion of parties that had content on pages
Pop-up that informs of the use of cookies	4/9
Terms and conditions for use of the website	9/9
Number of third-party cookies on the landing page	Between one and six on the landing page [39]
Cookies from Facebook	5/9
Cookies from Google Analytics [40]	8/9
Google DoubleClick [41]	1/9
Anonymize-IP for Google Analytics [42]	3/9
Stores the IP address of the visitor	6/9

Like the great majority of website owners, Norwegian political parties track activity on their own web pages by using cookies. Cookies are small files that are stored on the visitor's own device, which then recognise and track the visitor from one visit to the next. The most common cookie is Google Analytics, a free software that analyses the behaviour of visitors to websites. Google Analytics is ostensibly free; however, Google earn revenue from the personal data the company receive through the websites. Personal data is at times anonymized during further processing by Google. It is the owner of the website itself that decide whether the anonymizing function is selected. In our review of the websites, it has not been possible to evaluate if the anonymizing function was used, only if it had been stated in the website terms and conditions. This is especially true for websites using Google Tag Manager.

A majority of the parties have installed third party cookies from Facebook. These cookies send information to Facebook about how the user has used the political parties' websites. One of the cookies from Facebook also collects information about users of the web pages that are not registered Facebook users.

Our survey showed that the parties mainly use cookies from Google and Facebook. A majority of the parties have also given other third-party agencies access to their website via cookies. These third-party agencies are granted access to information concerning visitors, without the parties themselves being able to keep track of where this information ends up and what it is used for.

In the interviews, some uncertainty and lack of oversight was revealed concerning the cookies and tracking images used. In addition, several parties stated that they had installed cookies they did not use. The cookies can, however, collect information that is sent to third parties.

According to the GDPR, information must be provided concerning the processing of personal data when a user opens a website. With some exceptions, we found that the information provided is adequate; however, there is room for improvement.

Who do the parties cooperate with?

There are a number of companies that offer services pertaining to data collection and data analysis to Norwegian political parties. From a privacy perspective, it is important that the responsibility for processing of data is clear, so that data is responsibly processed, and

[39] A "landing page" is the first page viewed when visiting a website.

[40] Cookies from Google Analytics do not appear as a third party, rather as a cookie from the party's website.

[41] Google DoubleClick is an advertising function that can follow you across websites.

[42] Anonymize-IP for Google Analytics anonymizes the visitor's IP address in connection to further processing by Google. Complete IP addresses are thus not registered.

that it is clearly stated who is responsible for how the data is used.

Companies that offer data analysis have different approaches to the targeting of political messages. Bisnode, which offer political targeting services in Norway, has stated that they are going to take "an ethical time-out" in the local government elections in 2019. This means that they will not be providing data analysis to political parties for profiling purposes. This is in line with the advice provided by the United Kingdom's Information Commissioner's Office.[43]

All of the parties, except for one, stated that they purchased services from external companies during the election campaign. These companies assisted the parties in building target groups, driving data analysis and organising and targeting digital campaigns. It emerged during the interviews that it is the external companies that are chiefly responsible for identifying and defining segments and target groups to which the parties can send political advertisements or contact during door-to-door canvassing.

Several of the parties, particularly the smaller ones, did most of the work involving advertising on Facebook themselves. One party stated that they did not purchase services from external agencies during the election campaign, while another stated that they mainly worked with freelancers. **The parties relate to the advertising industry in different ways, and therefore have different access to data analysis and defined target groups.**

Most of the companies mentioned in the interviews are based in Norway. This included several marketing agencies, but also public institutions such as Statistics Norway, which among other things provides basic constituency data. Some of the companies also have offices in North America. It was unclear during the interviews as to how many of the external companies used subcontractors.

What are the conditions that impact the parties' use of digital targeting technology?

The parties' take on data analysis and targeting of political messages is greatly affected by the internal and external conditions they must adhere to.

We found that key framework conditions for the parties are economics, competence, trust in the political system and the effectiveness of targeting.

Party finances

It emerged from the interviews that economic resources is the condition that most restricts how the parties utilise various targeting methods. All the political parties we interviewed stated that they either do not have sufficient resources for extensive targeting, or that they have to limit the extent of their data analysis and digital targeting in light of their available resources. For example, the parties' election campaign budgets are not sufficient for them to request advertising agencies to continuously design alternative versions of the same advertisement so that they can be targeted to different groups.

We also found that personnel resources and competence within the party organisation itself influence the types of tools and services used during campaigns.

To shed light on the economic framework the parties operate in, we have compiled publicly available data on election campaign budgets.[44] The table on the following page shows the economic resources used for the budget post "Campaign expenses – marketing initiatives".[45]

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

[44] In Norway, there is a high level of transparency in party financing, and all political parties must report on their accounts and contributor information. Statistics Norway, on behalf of the Ministry of Local Government and Modernisation, compiles this information and makes it publicly available on the website partifinansiering.no.

[45] The dataset from partifinansiering.no does not contain figures for the Progress Party *[Fremskrittspartiet]* under the item "Campaign expenses – marketing initiatives".

Campaign expenses – marketing initiatives	
Labour Party *(Arbeiderpartiet)*	NOK 17 985 232
Conservative Party *(Høyre)*	NOK 14 329 067
Liberal Party *(Venstre)*	NOK 7 614 759
Green Party (*Miljøpartiet De Grønne)*	NOK 4 870 221
Socialist Left Party (*Sosialistisk Venstreparti)*	NOK 1 205 306
Christian Democratic Party *(Kristelig Folkeparti)*	NOK 830 622
Centre Party *(Senterpartiet)*	NOK 627 079
Red Party *(Rødt)*	NOK 260 943

The economic resources that are allocated to "campaign expenses – marketing initiatives" in the budget do not necessarily correspond to the resources that are actually used. However, the table indicates that the budgets are moderate and that economic resources vary between the parties. At the same time, several of the parties expressed concern that the economic differences between large and small parties will become more evident in the digital election campaign. Many of the parties stated that the two largest parties had more resources available to run a digital election campaign.

International research indicates that economic resources place limits on the use of microtargeting in other countries as well. Researchers that have examined the use of targeting technology in relation to election processes in the Netherlands and Germany point out that modest budgets restrict the use of this technology.[46] In other words, in line with what other parties experience in Europe, Norwegian parties are naturally restricted by modest budgets.

The relatively modest election campaign budgets function as an effective barrier against extensive microtargeting of political advertising.

Competence and skill

In many of the parties there is limited formal competence and skills relating to the use of advertising and analysis tools. It is common in Norway that external cooperating partners process data on behalf of the parties. In one of the interviews, we were informed that this created some concern that the election campaign was becoming increasingly professionalised, and it is more difficult to have adequate competence for digital marketing within the party.

A few parties have employees with key competence in digital marketing, and have been able to develop "home-made" solutions that improve efficiency in activities such as door-to-door campaigning. However, it is a common factor in most of the parties that external agencies carry out data analysis and establish target groups that the parties can send digital advertising to or visit at home.

Trust

In our interviews, the parties had the common attitude that they would not go too far in advertising aimed at small target groups. In addition to legal issues, several of the parties stated that they are dependent on the trust of their voters, and infringements against that trust can negatively impact the organisation's reputation.

The political system

The Norwegian political system differs from the systems in the US and the United Kingdom, where there has been widespread use of microtargeting techniques in election campaigns. In Norway, we have a multi-party system, in which there are several parties that set the agenda with a greater consensus on key policy areas.

In a multi-party system, such as in Norway, parties must take into consideration that they will likely have to form coalitions and make compromises after the election. In a two-party system, it is more of a case of "win or lose". This type of political system is more vulnerable to polarisation and entrenchment, which in turn can make micro-targeted messaging more effective.

Scepticism towards digital targeting

[46] See Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. H. (2017). Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. *Internet Policy Review, 6*(4), and Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political microtargeting in Germany. *Internet Policy Review, 6*(4).

The parties consistently stated that digital targeting in an election campaign context do not represent a revolution that has made traditional forms of campaigning obsolete. Several of the parties mentioned that meeting voters face-to-face was prioritised and still viewed as the best way to increase support. When questioned as to whether the parties would use digital platforms *more* or *less* in future elections, opinions were divided. One party responded that it would make greater use of digital platforms in future election campaigns, while another party stated it would reduce its use of digital platforms, relying more on meeting voters personally. The remainder of the parties did not provide any clear response to this question. None of the parties stated that they would cease altogether the use of digital platforms or data analysis in election campaigns.

Scepticism towards the extensive use of microtargeting of political messaging will be affected by the conditions the parties must adhere to – and these conditions may change. With larger election campaign budgets, cheaper data analysis technology and more polarised political arguments, there may potentially be less scepticism towards microtargeting.

Challenges and risk factors

Even though Norwegian political parties are careful in their approach to microtargeting, there are certain challenges and risks that the parties, in varying degrees, are aware of and must deal with.

Many of the parties believe their opportunities are defined more by the limits that tech companies set for them than by their own established routines. When questioned on how closely the parties focus their segmenting of target groups on Facebook, several responded that *"they did not go any further than what Facebook permit"*. This type of attitude can be something of a pitfall. Facebook has introduced restrictions within its advertising tools as a direct consequence of political pressure, in the wake of a number of scandals in recent years. These restrictions are not necessarily introduced to comply with Norwegian legislation, and legal and ethical evaluations of political operators should be done independently of the opportunities a platform offers.

Facebook, and other digital platforms that earn revenue from the sale of digitally targeted advertisements, have financial incentives to provide the most effective targeting technology to their clients. Decisions regarding properties and functions in advertising tools offered by these companies are made in private boardrooms thousands of miles away, and do not necessarily take into consideration the well-being of Norwegian democracy.

Some of the parties have also experienced pressure from companies trying to sell them products and solutions – often based on extensive targeting that may be in conflict with both legislation and ethical boundaries. Even though the parties are currently resisting solutions that cross these boundaries, it is unlikely that the pressure from providers will lessen in the future.

It is highly likely that targeting technology will become cheaper as the pace of technological development increases. This means that the restrictions that naturally arise due to limited budgets may not exist to the same extent in two, four or six years.

Even though there is significant awareness about the problematic sides of the use of personal data in political campaigns, none of the Norwegian parties have formalised guidelines for this type of use. This means that some of the boundaries set by election campaign leaders may change due to organisational changes, such as when a new person takes over the job.

Several parties also expressed concern for the role of private companies in a digitalised and data-driven election campaign. Furthermore, representatives from three parties expressed concern that actors and groups that are not political parties, or appear to be partially anonymous, can have an extensive range and impact. This concern was raised in context with the fear of increased polarisation and relativism of facts. **If the parties experience that they are competing against actors that do not follow the rules, a situation may arise where the boundaries for acceptable use of microtargeting technology are moved.**

In an election campaign, a political party will fight a tough battle to persuade the voters and win the power to lead our society. For some parties, this means gaining or maintaining power in government. For other parties, it can be a question of political survival. For many politicians, election results determine the position they hold, which is the same for the employees of the party organ. The risks highlighted above must be viewed in light of how much is at stake when parties go out to secure votes.

Conclusion

Privacy legislation places restrictions on how far political parties can go in their quest for votes. Information on a person's political views is given particular protection in privacy legislation. The European Data Protection Board has also drawn up guidelines that specifically address the use of personal data in the context of election campaigns.

The Cambridge Analytica scandal showed how advanced technology, coupled with huge amounts of personal data, can be exploited to become a powerful tool used for political influence and manipulation. The campaign for Brexit, as well as the campaign that led Donald Trump to the White House, are very likely to be examined and investigated for many years to come. Our report shows that the current status quo is rather different in Norway:

- Norwegian parties are cautious in their use of microtargeting and consistently restrict their use of invasive targeting. This caution must be viewed in light of a number of conditions, both economic and social, with which the parties must comply.
- Facebook is the central tool for the digital advertising of political messages, and the parties use mainly demographic data to target voters.
- Certain parties include interests and behaviour in their targeted advertising on Facebook, as well as in their programmatic advertisements.
- None of the parties we interviewed stated that they use their own party data, such as member lists, email addresses and telephone numbers, to create target groups in Facebook. Even though some parties have done so previously, this appears to be a boundary that no party currently want to cross.
- Digital platforms play a key role in election campaigns; however, traditional forms of campaigning, such as door-to-door canvassing and campaign stands, are still given high priority.
- The parties are increasingly reallocating advertising resources from newspapers to digital platforms. These platforms allow for more detailed targeting.
- In general, there is a lack of awareness concerning the use of cookies found on the parties' websites. Cookies not actively used by the parties can still send information to third parties.
- Door-to-door campaigns are increasingly organised with the assistance of targeting technology. Innovation in this field is high; however, the use of this type of technology varies from party to party.
- A party's innovative tempo is largely restricted by economic resources. Advanced, digital election campaigns using extensive numbers of advertisements aimed at narrow segments are too costly for Norwegian parties, and parties do not always see it as necessary to send targeted or specially tailored advertisements to narrowly defined target groups.

Even though we do not find that Norwegian parties have the necessary conditions, resources or the need for this type of finely filtered microtargeting that could have formed the basis for an "Oslo Analytica", there are vulnerabilities and risk factors.

- None of the parties have established written guidelines for the use of personal data and digital microtargeting. Such guidelines could potentially make the parties less vulnerable in the event of replacement of personnel and when purchasing services associated with targeting and data analysis.
- Many of the parties adhere to the framework of foreign companies and their use of targeting technology. It is not necessarily the case that these frameworks comply with Norwegian or European legislation.
- The technology used to target advertisements represents major privacy challenges, since personal data is not treated in an open and transparent manner. Political parties have a greater responsibility than commercial actors when utilising this type of technology, as the consequences of a non-transparent and non-compliant marketing of politics can lead to an erosion of trust in the political system.
- The conditions that presently contribute to restricting the parties' use of microtargeting may change. This may contribute to microtargeting becoming more extensive in the future. For example, election campaign budgets may increase and targeting technology may become cheaper and more user-friendly.

Six recommendations for the use of microtargeting of political messages

As we have seen in this report, targeting of political messages presents challenges in Norway. In light of this, we have formulated six recommendations for political parties to consider when using digital targeting technology:

1. Parties should collaborate to create codes of conduct that stipulate a common framework for the parties' use of personal data, both in an election campaign context and in general. A central framework should be established that stipulates clear internal boundaries on how far digital targeting can go. These boundaries must be communicated both to new employees and to the external agencies that services are purchased from during the election campaign. Local constituencies, regional groups and local politicians must be made aware of these boundaries.

2. Political parties are themselves responsible for how political messages are advertised. The parties must therefore evaluate which data they believe is necessary to use to engage the voters, and independently assess what is legally and ethically defensible, and not entrust this decision to third parties. This is the core responsibility in data processing, according to the GDPR. The opportunities offered by a digital platform may be in conflict with regulations.

3. Parties must be aware of the fact that information about a person's political views is a special category of personal data, and is thereby given special protection by the GDPR. Derived data is also considered to be personal data. The more finely filtered, and the closer the party gets to assume a person's political views, the more likely it is that this involves processing of information of a person's political views.

4. Political parties must acquire an overview and take responsibility for the type of information that is collected from their websites. Even though the parties themselves do not utilise the information collected by installed cookies, personal data is sent on to third parties such as Facebook and Google.

5. The parties must ensure that applications and technology used in connection to door-to-door canvassing comply with relevant regulations. If analyses are purchased from an external agency that provide the address of persons with a given voter profile, this will in many cases involve the processing of personal data.

6. There must be a clear demarcation of responsibility when political parties purchase services from external providers. The parties must clarify this responsibility and ensure that they have a data controller agreement if the external provider is to process personal data.

References

Autoriteit Persoonsgegevens. (2019, 15. februar). Verkennend onderzoek naar gebruik persoonsgegevens in verkiezingscampagnes. Hentet fra https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennend-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes

Bartlett, J., Smith, J., & Acton, R. (2018). *The Future of Political Campaigning*. Demos. Hentet fra www.demos.co.uk

Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R., & Wright, G. (2019). *Personal Data: Political Persuasion. Inside the Influence Industry. How it Works*. Tactical Tech. Hentet fra https://tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf

Belli, L. (2018, 5. desember). WhatsApp skewed Brazilian election, proving social media's danger to democracy. *The Conversation*. Hentet fra http://theconversation.com/whatsapp-skewed-brazilian-election-proving-social-medias-danger-to-democracy-106476

Bennett, C. J. (2016). Voter databases, microtargeting , and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law, 6*(4), ss. 261-275. doi:https://doi.org/10.1093/idpl/ipw021

Bodó, B., Helberger, N., & de Vreese, C. H. (2017). Political microtargeting : a Manchurian candidate or just a dark horse? *Internet Policy Review, 6*(4). doi:10.14763/2017.4.776

Cadwalladr, C. (2017, 25. november). Vote Leave donations: the dark ads, the mystery 'letter' – and Brexit's online guru. *The Guardian*. Hentet fra https://www.theguardian.com/politics/2017/nov/25/vote-leave-dominic-cummings-online-guru-mystery-letter-dark-ads

Cadwalladr, C., & Graham-Harrison, E. (2018, 17. mars). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Hentet fra https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Chase, J. (2018, 1. mars). Deutsche Post sold voter microtargeting data to CDU and FDP. *Deutsche Welle*. Hentet fra https://www.dw.com/en/deutsche-post-sold-voter-microtargeting-data-to-cdu-and-fdp/a-43218488

Chester, J., & Montgomery, K. C. (2017). The role of digital marketing in political campaigns. *Internet Policy Review, 6*(4). doi:10.14763/2017.4.773

Commission Nationale de l'Informatique et des Libertés. (2016, 8. november). *Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?* Hentet 7.5.2019 fra https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

Datatilsynet. (2015). *Det store datakappløpet: Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet*. Hentet fra Det Store Datakappløpet: https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/kommersialisering-norsk-endelig.pdf

Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. H. (2017). Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. *Internet Policy Review, 6*(4).

Duportail, J. (2018). *The 2017 Presidential Election: The arrival of targeted political speech in French politics*. Tactical Tech. Hentet fra https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-france.pdf

European Data Protection Board. (2019, 13. mars). *Statement 2/2019 on the use of personal data in the course of political campaigns*. Hentet fra edpb.europa.eu: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

Faizullabhoy, I., & Korolova, A. (2018). *Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions.*

Ghoshal, D. (2018, 28. mars). Mapped: The breathtaking global reach of Cambridge Analytica's parent company. *Quartz*. Hentet fra https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/

Gibson, R. K., & McAllister, I. (2015). Normalising or Equalising Party Competition? Assessing the Impact of the Web on Election Campaigning. *Political Studies, 63*(3), ss. 529-547. doi:https://doi.org/10.1111/1467-9248.12107

Goldman, R. (2018, 21. desember). *Changes We Made to Ads in 2018*. Hentet 30.4.2019 fra Facebook Business: https://www.facebook.com/business/news/changes-we-made-to-ads-in-2018

Hersh, E. D. (2015). *Hacking the electorate. How campaigns percieve voters*. Cambridge University Press.

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

Kelion, L. (2018, 11. juli). Emma's Diary faces fine for selling new mums' data to Labour. *BBC News*. Hentet fra https://www.bbc.com/news/technology-44794635

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), ss. 5802-5805. doi:https://doi.org/10.1073/pnas.1218772110

Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political microtargeting in Germany. *Internet Policy Review, 6*(4). doi:10.14763/2017.4.780

Le Monde. (2016, 17. november). La CNIL enquête sur Knockin, l'application des militants sarkozystes. *Le Monde.* Hentet fra https://www.lemonde.fr/politique/article/2016/11/17/la-cnil-enquete-sur-knockin-l-application-des-militants-sarkozystes_5032818_823448.html

Lotame. (2017, 4. oktober). *The Benefits of Cross-Device Marketing*. Hentet 2.5.2019 fra Lotame.com: https://www.lotame.com/benefits-cross-device-marketing/

Merrill, J. B., & Tobin, A. (2019, 28. januar). Facebook Moves to Block Ad Transparency Tools — Including Ours. *ProPublica*. Hentet fra https://www.propublica.org/article/facebook-blocks-ad-transparency-tools

Nes, C. (2019, 24. januar). Høstens valgkamp blir trolig den mest teknologisk avanserte noensinne. Dagens Næringsliv. Hentet fra https://www.dn.no/politikk/personvern/malrettet-annonsering/datatilsynet/teknospaltist-hostens-valgkamp-blir-trolig-den-mest-teknologisk-avanserte-noensinne/2-1-526848

O'Brian, C. (2018, 14. juli). How NationBuilder's platform steered Macron's En Marche, Trump, and Brexit campaigns to victory. *Venturebeat*. Hentet fra https://venturebeat.com/2017/07/14/how-nationbuilder-helped-emmanuel-macron-secure-a-landslide-in-frances-legislative-elections/

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, 17. mars). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Hentet fra https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Ross, T. (2015, 16. mai). Secrets of the Tories' election 'war room'. *The Telegraph*. Hentet fra https://www.telegraph.co.uk/news/politics/11609570/Secrets-of-the-Tories-election-war-room.html

Schiff, S. C. (2018, 6. desember). *Increasing Ad Transparency Ahead of India's General Elections*. Hentet 30.4.2019 fra Facebook Newsroom: https://newsroom.fb.com/news/2018/12/ad-transparency-in-india/#

Solon, O. (2018, 16. Mai). Cambridge Analytica whistleblower says Bannon wanted to suppress voters. *The Guardian*. Hentet fra https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony

Svaar, P., Fossen, C. H., Tomter, L., Andersen, K. A., & Ertesvåg, O. R. (2018, 26. juni). Høyre rangerte tusenvis av nordmenn etter hvor sannsynlige Høyre-velgere de var. *NRK*. Hentet fra https://www.nrk.no/norge/hoyre-rangerte-tusenvis-av-nordmenn-etter-hvor-sannsynlige-hoyre-velgere-de-var-1.14089573

Svaar, P., Husabø Fossen, C., Tomter, L., Gisetstad Andersen, K. A., & Ruggesæter Ertsvåg, O. (2018, 21. juni). Høyre granskes av Datatilsynet: Lastet opp medlemsdata til Facebook. *NRK*. Hentet fra https://www.nrk.no/norge/hoyre-granskes-av-datatilsynet_-lastet-opp-medlemsdata-til-facebook-1.14090299

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday, 19*(7). doi:https://doi.org/10.5210/fm.v19i7.4901

Waterson, J. (2019, 27. januar). Facebook restricts campaigners' ability to check ads for political transparency. *The Guardian*. Hentet fra https://www.theguardian.com/technology/2019/jan/27/facebook-restricts-campaigners-ability-to-check-ads-for-political-transparency

Willsher, K., & Henley, J. (2017, 6. mai). Emmanuel Macron's campaign hacked on eve of French election. *The Guardian*. Hentet fra https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election

Datatilsynet

Office address:
Tollbugata 3, 0152 Oslo,
Norway

Postal address:
Postboks 458 Sentrum
0105 Oslo, Norway

postkasse@datatilsynet.no
Telephone: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet