Teknologirådet

Elections, technology and political influencing

The new political campaign

Social media and digital tools have changed how political campaigns are organized and run. This is particularly relevant in two areas:

- Political messages can be targeted toward individuals far more effectively than ever before and the potential to reach large voter masses is huge.
- The digital tools are global and easily accessible, which makes it possible for foreign actors to influence voters.

Social media is a tool that can strengthen communication and the public conversation. After Obama's 2008 campaign, social media was seen as a democratizing tool allowing direct communication with voters and with an infrastructure lowering the bar for political involvement.

However, recent years has shown that the same digital tools can be used to secretly manipulate voters, as well as spreading fake news and disinformation.

The technology of campaigning

Today, a political campaign can be fully organized online. Digital tools are readily available, require almost no preexisting knowledge, and can save time and effort through automation. Using social media, the political parties can acquire personalized advertisements, monitor public response to their posts, test and gather data to continuously make improvements.

SUMMARY

» Political advertisement on television is illegal but allowed online and in social media.

» Political campaigning has gone from aiming at wide target audiences to personalized influence through social media.

» In recent years, third-party actors have used these tools to influence voters by spreading misinformation and fake news.

» Several countries are now mobilizing to stop voters from being manipulated ahead of elections.

From target groups to individuals

Methods and technology developed in the digital advertising industry are now used at large scale in political marketing. When we use online services a number of actors monitor our activity. They collect data which provides a very detailed mapping of our lives. The data is then analyzed to offer personalized products and services.

Political advertisements on social media have become standard, and ahead of the Brexit-vote in 2016, the Vote leave-campaign published around one billion targeted ads, mainly through Facebook.

Ads are often targeted based on a combination of demographic information such as gender, age, where you live, marital status, health conditions, or your workplace.

Additionally, Facebook can create categories based on derived information, such as your perceived political affiliation or ethnic background, without you ever having given that information.

Testing and improving

With marketing tools one can follow the response on ads in real-time. This makes it possible to experiment with different messages on various groups, and then spread the ads that creates most engagement and reach the largest crowd.

In the 2016 U.S. presidential election, the Trump campaign posted 5,9 million different ads on Facebook. They tested a variety of ads and spread the ones that were liked and shared the most, along with ads leading to donations. In comparison, the Clinton-campaign only published 66 000 different ads.

An "Office-suite" for elections

Nationbuilder is a complete toolkit to run digital campaigns and includes work coordination, administrating websites and social media, financing, and distributing targeted marketing.

The software is used all over the world and has around 200 customers in Great Britain alone. Thus, parties and organizations have access to both data and powerful tools without being experts in the area.

Automated accounts

Automated social media accounts, commonly known as "bots," makes it possible to publish immense amounts of content in a short amount of time. Such bots have increasingly been used to spread misinformation and fake news, right before elections.

During the first six months of 2018, Twitter deleted more than 200 million accounts for spam or illegal automation.

The 2018 Swedish election saw a dramatic upsurge in Twitter-bots sharing political content. Most of this content came from websites publishing fake news.

CODE OF CONDUCT

Both Canada and Great Britain are discussing codes of conduct digital campaigning. The Norwegian Board of Technology suggests that Norwegian political parties should consider the following:

Openness and labeling

The political parties must be open about how they use data and place labels on online- and social media ads. The labeling can include information about how much money has been used, and who is in the target group. Political ads should also be stored in an archive.

A budgetary rule for data and money

The parties should in unison determine what types of data can be used for targeted political advertisements. They should also decide whether there needs to be introduced a spending limit for digital marketing.

Campaign audits

The parties must disclose how much money was spent on digital marketing and how this money was spent. Data audits should be introduced as a way of ensuring that data is only used for its intended purpose.

From campaigning to manipulation

In Norway, political marketing is regulated. Political TV advertisements are illegal based on the rationale that television has too significant of an impact and can give a skewed image of complicated issues that favors the parties with the most financial resources.

On the other hand, there are no regulations for political advertising online. Recent studies have shown that social media ads have a significant effect on voters, and political parties are allocating increasingly larger shares of their marketing budgets toward digital platforms.

Global industry

In 2017 it was discovered that the company Cambridge Analytica had access to data from 87 million Facebook users. Cambridge Analytica supported Donald Trump in his campaign by offering psychometric profiling of these users.

There are more than 250 companies specializing in the use of personal data in political campaigns. Although the examples from the elections in the U.S. and Great Britain have received the most coverage, there are examples from France, Brazil, Kenya, and India that show companies like Cambridge Analytica can be found all over the world.

After the Brexit vote, multiple investigations on how personal data is used to influence voters have taken place. The British Information Commissioner have already given multiple fines for illegal use of personal data.

For example, a company that offers counselling services to pregnant women and parents with young children sold a million of their users to a data broker. This data was then used by Labour to personalize political ads to new mothers before the 2017 election.

Who forms our opinions?

The news feed on social media is controlled by algorithms. We see what the algorithm thinks we want to see based on our interests, beliefs and attitudes, and posts from friends we frequently interact with. Posts that engages people via shares, comments, and "likes" are spread quickly.

This way we are very rarely exposed to opinions and attitudes that challenge our own. In turn, this can reinforce existing beliefs and contribute to further distancing from other groups. Getting frequent confirmation on one's own beliefs creates an illusion that these beliefs are more common than they really are – a phenomenon known as echo chambers.

Targeted marketing can also contribute to this. "Dark ads" are ads that are only shown to the target audience. This means that parties can select what messages they want certain groups to see, without their knowledge that this is happening. Different people and groups can thus get different impressions of a party's political message.

Disinformation

Digital marketing tools are global and easily accessible. This opens the opportunity for foreign actors to influence voters using the same methods and technologies as political parties without being noticed. Though determining the concrete effect is difficult, several investigations have shown that the reach of influencing campaigns is significant.

External influence

Multiple reports have concluded that the Russian Internet Research Agency (IRA) used social media to influence American voters. From 2013 and onto today the IRA has reach millions of Americans via Facebook, Instagram and Twitter. IRA operated as a professional digital advertising firm with its own logos, personas, and typography.

Even though the IRA's activity was exposed it did not stop. Since the 2016 election, particularly Instagram has seen Russian accounts increasingly attempting to create public engagement around topics such as national security and issues especially important for young voters.

In India, disinformation spread via WhatsApp has led to multiple violent incidents. Unlike the U.S., disinformation is not spread by foreign actors, but through domestic environments. Because WhatsApp is encrypted, users and groups cannot be monitored as closely as on Facebook and Twitter, which makes it more difficult to expose the actors behind it.

IRA's activities in the U.S. are probably the most well-known example. However, influencing campaigns have been identified in numerous countries. There are particularly three commonly used reoccurring strategies:

Passivation

Russian IRA focused much of their efforts towards urging African American voters not to vote. The posts encouraged the group to boycott the election and provided false information on voter registration procedures.

Generate confrontation and polarization

Ahead of the 2018 election in India, large quantities of false newspaper headlines were shared in WhatsApp groups as an attempt to create polarization between Muslims and Hindus. Especially the Congress Party was portrayed as anti-Hindu.

In May 2016, the Russian IRA organized both a demonstration and a counter-demonstration on the same subject matter via the Facebook-groups "Heart of Texas" and "United Muslims of America."

Spreading fake news

Several Twitter-bots spreading fake news were created ahead of the Swedish election in 2018. Due to the high activity by these bots, the content was quickly spread, liked, and shared by regular users. Swedish Twitter-users are some of the most frequent sharers of disinformation in Europe.

Measures against manipulation

As a result of the recent exposure of voter manipulation, several measures aimed at hindering voter manipulation have been initiated.

Self-regulation for the Internet giants

Following an initiative from the EU-Commission, the largest internet companies and actors from the advertising industry have created a "Code of Practice on Disinformation." The aim is to generate more transparency around political ads (i.e. who sent it and how it was financed), hinder misuse of bots, and prioritize credible information in the news feeds.

Twitter, Facebook and Google have already begun labeling political advertising, making it easier for users to distinguish ads from other content.

Both Twitter and Facebook have created an archive for political ads. To stop foreign influencing, Facebook have placed restrictions on who can purchase political advertisements, limiting it to domestic actors.

However, this action has been problematic in the EU as several institutions are campaigning across country borders ahead of the EU election. Consequently, as the EU-Commission is in Brussels, they can really only promote information regarding the election to people who live in Belgium.

The Internet companies are also working on better exposing and deleting automated accounts spreading illegal content. From January to March 2019, Twitter identified 40 million accounts as spam or illegally automated accounts. In March 2019, Google deleted one million YouTube accounts for violating rules for spam, misguiding content, and fraud.

Statutory responsibility

Several countries, including Germany, France, and Italy, have taken legal measures to emphasize social media companies' responsibility for the content posted on their platforms.

For example, legislative changes have demanded a response time for deleting illegal content, which makes it possible to fine actors that do not follow this. In Germany, all illegal content must be removed within 24 hours. This form of regulation has been criticized because other lawful content, such as satire, are being removed in the process, arguably limiting freedom of speech.

Cyber defense for democracy

The EU has created a notification system that enables member countries to quickly share information if they notice attempts to manipulate election processes, and meet to respond concordantly.

Sweden is considering establishing a new authority responsible for developing the country's psychological defense. Australia and several other countries have already created their own units aiming to protect the countries' voters from foreign influencing.

Information and awareness

Several strategies focus on making voters aware that they can be manipulated:

- Fact-checkers, such as faktisk.no, evaluate news articles and statements, in order to disclose disinformation and fake news.
- Credibility tools, like Le Décodex and NewsGuard, examine online newspapers and other sources. They look at websites history of posting disinformation and give them a credibility score.
- Swedish Civil Contingencies Agency (MSB) has written a handbook for how to approach and identify disinformation. The handbook is translated and used in multiple countries.

Authors: Tore Tennøe / Marianne Barland

Kontakt: post@teknologirådet / www.teknologiradet.no

The Norwegian Board of Technology (NBT) advises the Norwegian Parliament and Government on new technology.