WHERE IS THE HARM IN MICROTARGETING AND HOW DOES IT IMPACT DEMOCRACY?

Microtargeting is the strategy used to create highly specific advertisements to narrowly-targeted groups or individuals. Microtargeting is more commonly called online behavioural advertising in advertising and marketing studies, sometimes also called profiling or behavioural targeting, "political behavioural targeting" (PBT) in political marketing studies, or news personalisation in journalism.

We use all terms interchangeably here.

These are **positive aspects of microtargeting**:

- It uses the audience insight gleaned to tailor content even more precisely, thus increasing both efficiency and effectiveness. For example, a study by Metcalf, Angle, Phelan, Muth, & Finley (2019) found a significant influence of a normative message among random (nonmicrotargeted) prospects, increasing response by 23% over the control group.

- *PBT* could increase political participation through a more relevant political information or political ads for specific audiences, or it might reach citizens who are difficult to reach through legacy. T*ailored messages might be understood as more personally relevant. Thus, politics may be perceived as less abstract. Political micro-targeting could hence result in engaging citizens previously not politically active. Microtargeting could also have an empowering effect for niche political parties.*

Source: Pixabay.com

These are **negative aspects of microtargeting** (sometimes included among the broader concept of "online manipulation", see Susser, Roessler, & Nissenbaum, 2019)*:*

- It exploits personal data without previously informed consent. For example, Belgian, Spanish and Irish authorities received complaints that Google does not respect GDPR. In the Irish case, Google has been accused of using digital advertising auctions that violate users/consumers´ rights. Specifically, Google was accused of secretely using hidden webpages that feed the personal data of its users to advertisers, without sufficient control or concern over data protection (Murgia, 2019).

- It blurs the boundary between advertising and other forms of online content. For example, in an exploratory study, Meyer *et al* (2019) found high rates of mobile advertising through manipulative and disruptive methods in free and paid apps in the 5 (years old) and under category on the Google Play app store. Of the 135 apps reviewed, 129 (95%) contained at least 1 type of advertising.

- It allows for the spreading information disorder and other social media harms.

- *There is a risk of fragmentation of the public sphere, and the strengthening or creation of new digital divides - ideological "bubbles" or* echo chambers.

- *It can commercialise political campaigns to the extreme, turning politics into business motivated and emotionally driven exercise (see* Baldwin-Philippi, 2019). *Moreover, Facebook, Twitter, and Google go (or used to go) beyond promoting their services and facilitating digital advertising buys, actively shaping campaign communication through their close collaboration with political staffers. Kreiss and McGregor (2018) show that representatives at these firms serve as quasi-digital consultants to campaigns, shaping digital strategy, content, and execution.*

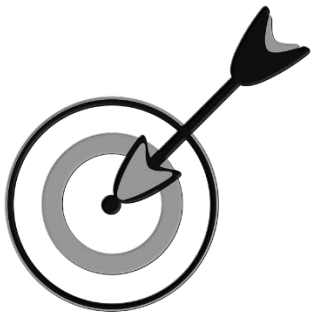
All these negative aspects have in common that they may violate its target's autonomy (Susser, Roessler, & Nissenbaum, 2019). The most infamous example of negative aspects of microtargeting is the Facebook/Cambridge Analytica scandal. Dobber, Trilling, Helberger, & de Vreese (2019) findings show that the potential for undesirable voter behavior (e.g. inability to deliberate autonomously, chilling effects, voter mistrust is very real. However, Nenadic (2018), after review of available literature, claims that the existing evidence seems not to support the thought that microtargeting might have a devastating effect on democracy.

The best ways of regulating online microtargeting

Boerman, Kruikemeier & Zuiderveen Borgesius (2017) review of academic empirical studies shows that consumers understand little about online behavioral advertising and the related data use, and current transparency approaches are not very effective in increasing that

understanding. Similarly, Papakyriakopoulos, Hegelich, Shahrezaye, & Serrano (2018) suggest (referring to Strandburg), that regarding personal data for political microtargeting, the act of a user opting in, given a very long document of terms and conditions, where how personal data might be used is outlined in a short and general manner does not signify transparency, or actual consent. As a result, consumers or voters who do not understand how data are used for online behavioral advertising cannot make meaningful privacy decisions, argue Boerman, Kruikemeier & Zuiderveen Borgesius (2017). Pasquale (2017) and Larsson (2018) also call for the need to regulate consumer rights at a level that is not as strongly dependent on the consumers' individual awareness.

In response, *Larsson (2018) believes, perhaps too optimistically, that consumer protection authorities will find ways to utilise not only machine learning but also increasingly intelligent artificial agents to find and counteract inappropriate market behaviour. In other words,* ***cooperation of legal and computer scientific expertise would be required to tackle these issues.***



Source: Pixabay.com

Larsson (2018) also calls for ***closer cooperation between the data protection authorities and consumer protection focused authorities****. This cooperation would include audits or control of how data-driven and targeting software operates, in order for consumer protection authorities to develop the ability to assess – in-house or perhaps through outsourced expertise – what the combination of algorithms and use of big data sources are leading to, and to discover the use of erroneous data. However, this may be too difficult task. In view of* Rhoen and Feng (2018), ***the algorithms used to process big data are largely opaque to both controllers and data subjects:*** *if the output of an algorithm has discriminatory effects coinciding with sensitive traits because the algorithm accidentally discerns an emergent property, this may remain unnoticed. At the moment, there are no remedies that can prevent the discovery of sensitive traits from non-sensitive data.*

To defend privacy, Boerman, Kruikemeier & Zuiderveen Borgesius (2017) propose that policymakers should not merely aim for consumer empowerment but also for their protection. Most privacy laws have elements that aim to protect consumers. For instance, many laws require companies to secure the data they collect against data breaches, and in many countries the law has stricter rules for certain types of sensitive data, such as health-related data.

Within the EU, there is GDPR. It is based on presumption that data activities are illegal unless they have some sound basis (Hoofnagle, van der Sloot & Zuiderveen Borgesius, 2019). While the GDPR only protects EU citizens, its impact is bound to be global in nature, affecting any organization that targets the European market or provides services and hold personally identifiable information on EU residents (Li, Yu & He, 2019). **GDPR** demands that organizations should get user consent to collect data and "implement appropriate technical and organizational measures" to protect personal data of EU residents (Kaushik & Wang, 2018). However, this **apparently does not prevent microtargeting**. For example, Rhoen and Feng (2018) argue that **although the GDPR poses special requirements for the processing of sensitive data, yet it is not clear whether these requirements are sufficient to prevent the risk associated with this processing because this risk is not clearly defined.** Furthermore, t**he GDPR's clauses on the processing of—and profiling based on—sensitive data do not sufficiently account for the fact that individual data subjects are parts of complex systems**, whose emergent properties betray sensitive traits from non-sensitive data.

Thus, to defend privacy, perhaps **more and stricter rules are needed for online behavioral advertising,** suggest Boerman, Kruikemeier & Zuiderveen Borgesius (2017). There may be online behavioral advertising practices that society **should not accept** such as **tracking on websites aimed at children and the use of online behavioral advertising data for online price discrimination**, believe Boerman, Kruikemeier & Zuiderveen Borgesius (2017).

In addition, Zuiderveen Borgesius, Möller, Kruikemeier, Ó Fathaigh, Irion, Dobber, Bodo, Vreese (2019) suggest that policymakers should also **consider requiring more transparency regarding microtargeting from political parties, or more broadly, from politically or ideologically motivated communication by institutional actors.** Furthermore, Bodó, Helberger, and de Vreese (2017) argue that microtargeting research must develop a better understanding of regulatory frameworks around platforms, personal data, political and commercial speech that shape the use of microtargeting.

In news business, *Lafrance and Carlson (2017) recommend that* personalization should be a way to enhance news decisions made by editors, professionals committed to quality journalism as a crucial component of an open society.

Compiled by SCM