Microtargeting and Cambridge Analytica Case

Roma
via di Porta Pinciana 34
tel. +39 06 454 954 70
fax +39 06 454 954 76

Milano
via S. Pietro all'Orto, 17
tel. +39 02 87199502
fax +39 06 454 954 76

info@cmplaw.it
www.cmplaw.it

Victoria Eikevold
INTERN

Gaia Morelli
PARTNER
gaiamorelli@cmplaw.it

What is microtargeting?

A person's mind is easily manipulated, especially when it has been watched, processed, analyzed, and then only shown what it really wants to see, and that can often be something very different from the truth. The internet and what someone chooses to use it for is probably one of the best ways to get a sense of the preferences and interests of an individual. Microtargeting is based on monitoring our behaviors and providing us contents – most of the time being commercial, marketing, or messages to manipulate our will – which we might be more willing to receive, read, pay attention to. For example, the way you might click on cat videos on Facebook, the time you spend reading articles about animals, the way you scroll down to the images, can be processed and then you are shown exactly what you would want to see, like kittens for sale in your area. Sounds fairly innocent really, maybe even convenient. You get to see more of what you like and everyone is happy. The end? Not quite!

Videos, images, and opinions regarding politics has also entered the social media platform and in the aftermath of the last presidential election in the United States, microtargeting of people's political views and the ethics of using this information for political gain became a major debate.

Political propaganda has been around in one way or another for ages. It can be a healthy part of a functional democracy. Every candidate wants to win the faith of the people and should be given the chance to show what they're all about. Ideally, a candidate would want to reach the largest crowd possible, through speeches and posters… or in recent days, the internet!

Propaganda has historically been a tool used on a macro level, meaning that the message sent out to the public was the same for everyone. Now, instead, the intent is to make such message as personalized as possible, in order to say just as much as necessary to convince you to vote that candidate. This also means that not everything that the candidate promotes and believes is shared with you in these messages… because you might not like the candidate overall. Unless you research your information with other means, you never get the full picture.

This is why, microtargeting mostly affects those who have little previous knowledge and interest in the political climate from before. The less one knows about the situation, the more likely are they to believe what is put in front of them without questioning whether it is the truth or not.

What happened in the US?

Cambridge Analytica, a political consulting firm specializing in data analysis, sent out personalized advertisements to at least 87 millions of American citizens in preparation for the upcoming election through the means of the social network, Facebook. Someone who held strong beliefs in the Pro Life movement and strongly opposed abortion would be a target for advertisement promising stronger regulations and limitations for abortion rights. This is just an example, as any person with a strong opinion towards a certain issue would be fed information meant to convince them to vote for one candidate rather than the other, based on their own beliefs. Advertisements showing negative messages and fake news about the opposing candidate proved to also be an effective weapon on the road to victory.

So how was Cambridge Analytica able to do this? Cambridge Analytica released a

personality quiz app on Facebook that would pay the American people $2-5 to take it. What people were unaware of was that when you take the quiz, it allows the app to access not only your own information, but all your facebook friends' information as well, and this became a massive pool of people. The biggest crime committed here is that people allowed the app to access their own data, but that does not allow for a third party to harvest and use that information for further processing with undisclosed purposes. Cambridge Analytica did collect everything, and they also used it, a lot.

Cambridge Analytica's facebook quiz would be marked as illegal gathering and processing of personal data as the takers of the quiz only allowed the specific app access but never gave specific consent for Cambridge Analytica to use sensitive information for reasons of political propaganda.

Is it possible under the GDPR?

This is the most controversial example of microtargeting happening at a mass level. The microtargeting was centered around United States voters. However, the data were collected by a UK company and involved, overall, data of individuals from all over the world. How could that be possible in Europe? The data collection is in violation of the General Data Protection Regulation (GDPR).

(GDPR) entered into effect in 2016 and became enforced in all member states in May 2018. There was a set of rules before 2018, called Directive 95/46/CE, but this was made in 1995 and was therefore considered outdated as it did not take into account the technological advances that has happened in the last 20 years. The GDPR for short enforces, in summary, that the public and private sector needs legitimate reason for collecting data on citizens online activity as well as bank statements and personal information, and if for some reason it is collected, it can only be used when it has legitimate reasons to do so under the law. There are very few legal grounds that would allow this processing, and the rules governing the processing of particularly sensitive data are even more restrictive.

Paragraph 9 of the General Data Protection Regulation states that "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (article 9)." Although there are a list of exceptions where this rule would not apply, it is not acceptable for any private company to profile a person´s online history and use it to send political messages.

What happened in the UK?

The Member States Supervisory Authority are still investigating and defining the administrative fines obliged for the unlawful processing of data used for political objectives. However, in several countries elections are still being controlled and democracy is being undermined. If it is completely illegal in Europe to watch people's online activity for political gain, then that must mean that this has not happened here before? Not exactly.

The Leave campaign in the United Kingdom also used microtargeting with the collaboration with Cambridge Analytica as a tool to promote British citizens to vote to leave the European Union. Different ads were shown on websites such as facebook to different people, depending on their age, gender, political opinions, and many other

factors. People who were passionate about environmental issues could find ads telling them that the European Union prevents the UK from standing up against animal rights, while elderly citizens might see ads telling them that if the country stepped out of the union than money previously spent on the union could then go to building more NHS hospitals throughout the nation. The Observer reported that personal data was taken from one million British citizens. The United Kingdom is, for the time being, still a member of the European Union and Cambridge Analytica's involvement in the referendum is therefore considered to be a violation.

As far as privacy regulations goes, the GDPR states clearly that "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" and the controller should also be able to prove that the data subject had been explained exactly what the the information would be used for (article 7, GDPR). If Cambridge Analytica did process people's activity online to show ads that were pro Brexit, then they would have to be able to show that each and every person, not only the one taking the personality test, but all of their Facebook friends were aware of the processing and gave their specific consent to the use of sensitive data. It would be highly unlikely for this to be the case!

Cambridge Analytica has since shut down for what they themselves claim to be a result of not having any clients left as a result of negative media exposure. Their database has also been seized. However, this kind of processing is still happening. The supervisory Commission, including the UK's ICO and the Italian Garante, sent a request to the Working Party 29 (WP29) to take action with respect to processing through online platforms. The WP29 have created a Social Media Working Group in order to develop a long-term strategy on the issue.

Effects of advertisement

How effective is microtargeting, really? Are we actually naive enough to pick the leader of a country because a Facebook ad tells us to do so? Statistically, everyone is affected by advertising. People might think highly of their ability to reject ideas that are forced upon them but in a world where each person sees advertising as soon as they walk out the front door, open facebook, or turn on the TV, it is unavoidable. Electing politicians for a country is not just a logical and scientific choice for citizens, it is also deeply affected by emotions and someone's personal struggles. Immigration is an issue that is largely used for political campaigning, and the average voter is probably not going to read up on the statistics and they will likely not make a list of pros and cons of welcoming migrants. This is for sure one of the most controversial issues in Europe and in the United States. For the majority, it comes down to one's own perception and feelings such as fear, love, rage, etc. If the average citizen acts primarily because of an emotional response, and ads appeal to this, people are likely to respond accordingly.

Invasion of privacy and ethical issues

A person should be able to roam the internet freely without feeling like they are being watched. In all probability, most of us would not freely send an excel sheet with our browser history and details about what we tend to click "Like" on and almost certainly, we would not make a summary of ourselves as stating all our political opinions, interests, and other intimate details and then send it to a data collection company and say "Hey, do what you want with this! I don't care".

United Nations Human Rights' Office of the High Commissioner released an adapted

resolution called 'The Right to Privacy in the Digital Age' in December 2013, in which they discuss the threat of online surveillance and violations of privacy. The document calls for "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale". Meaning that even if the data analysis companies should be prosecuted not only for violating the GDPR, but also for violation of the basic human rights.

* * * * *

DISCLAIMER

This article provides general and non-original information and it does not constitute a legal advice or a provision of legal services. Any action or decision, if any, cannot be based on the information contained in this article but it shall be subject to a qualified counsel's opinion. CMP Law or the authors take no responsibility for the updating or validity of the information contained herein.