Facultad de Ciencias Humanas y Sociales
Grado en Relaciones Internacionales

Trabajo Fin de Grado

DATA USE AND ABUSE IN POLITICAL COMMUNICATION.

CAMBRIDGE ANALYTICA AND THE BREXIT CAMPAIGN, A CASE STUDY.

Estudiante: **Blanca Méndez Egea**

Director: Prof. Ariel James Trapero

Madrid, junio 2021.

INDEX

1. INTRODUCTION.

Technological advances in recent decades have driven the transformation of political campaigns. They have been increasing the use of more innovative methods through microtargeting or data mining for increasingly digitised communication. Despite the many advantages of new technologies, regulation of what can and cannot be done with them seems to be slower than these developments, leading to unethical situations and abuses. Among others, the concept of freedom of thought and democracy appear to be affected by these rapid changes.

Over the last decade we have seen how business models based mainly on digital marketing or digital communication have been gaining importance and are currently one of the sectors with the highest profits. At the same time, major political and geopolitical changes have taken place which, although they cannot be explained exclusively by the use of social networks as a means of communication, can be considered one of the propelling factors, above all, of polarisation and the rise of populism. Some of these major changes were the arrival of Donald Trump in the White House, and the UK's exit from the European Union. Both changes were fraught with controversy and the campaigns for both democratic processes continue to be investigated to this day.

The main common factor in the controversy surrounding the presidential election and referendum campaigns is the gathering, use and analysis of private data of millions of voters for the placement of personalised advertisements aimed at manipulating the audience to vote in favour of the campaign in question. All this was done without the knowledge of the users themselves, making the manipulation and processing of data unnoticed. Moreover, both campaigns were surrounded by concerns about possible foreign interference.

It is in this context that the subject of the study has been chosen with the aim of examining the methods used, in relation to data processing, by the Brexit referendum campaign in 2016. To do so, first of all, the objectives and research questions will be discussed, as well as the reasons that have led me to choose this particular topic.

Secondly, a review of the different theories and concepts that are essential for the understanding of the topic will be presented. Finally, the case study, the Cambridge Analytica scandal and the Brexit referendum, and the techniques used during the campaign of the latter will be analysed, after which the research questions will be answered.

2. OBJECTIVES AND REASONS.

2.1. <u>Why was the topic chosen?</u>

The choice to study practices related to the use of user data for political campaign communication stems from an interest in raising awareness of the magnitude of the moral problem they pose, and the danger they represent for the quality of our democracies. The world and geopolitics have changed considerably in recent years. New technological advances and new means of communication such as social networks bring great benefits to society in terms of connectivity and access to information, but they also present high risks for individuals if they are not properly regulated.

An example of this delay in adapting society and electoral legislation to new technologies is the Brexit campaign. This, as will be seen throughout this paper, combines the violation of the rights of data owners, illegal electoral strategies of overspending on digital communication, and the possible interference of external actors in the campaign. In addition, the Brexit process has a strong link with the development of my studies in the field of communication. The referendum took place the year in which I started this Double Degree in International Relations and Bachelor in Global Communication, the investigations on the events surrounding the campaign in favour of the United Kingdom's exit from the European Union have been developed throughout these years, and finally the latter has become effective in the year in which I finish this academic stage. Therefore, I could not find a better research topic, nor a more relevant one, than to analyse a trend in political communication practices that is having direct and clearly visible effects on our lives as Europeans and on our moral rights.

2.2. Main objectives of the study and research questions.

For all of the above reasons, this study aims to explain the functioning of these new political communication practices. In order to visualise these methods and their possible effects, a case study has been chosen on the so-called Cambridge Analytica scandal in relation to the Brexit referendum. The study will try to present the key facts about the case, the main actors involved in it and the effects that these practices could have had on the outcome of this democratic process. Once the case has been analysed, the aim is to reach conclusions on the ethical and moral dilemmas involved in the use of user data for practices such as micro-targeting advertising in a political context. The purpose of the study is therefore to identify the main disadvantages that exist for society as a result of these practices and thus create the necessary background for the creation of new policies to reduce the abuse of data.

Therefore, with these goals, the questions that this study will attempt to answer are the following: What moral or ethical dilemmas arise with the use of data analytics practices for targeted political advertising? Can these problems be reflected in the events that took place during the campaign in favour of the UK's exit from the EU prior to the 2016 referendum? And finally, what changes should take place in order to address these moral dilemmas?

2.3. Methodology.

The study will therefore be a desk study. It will use primary sources such as the conclusions from the investigation conducted by the Infromation Commissioner's Office of the United Kingdom on the 2016 Brexit pre-referendum campaign, and the witness statements pertaining to the case, these being Christopher Wylie and Brittany Kaiser.

On the other hand, in terms of the sources used to analyse the social and moral consequences of communication techniques based on data analytics, for the purpose of targeted advertising, we can highlight the studies carried out by Linda J. Skitka about the link between moral convictions and political behaviour, and the research of authors such as Christian Fuchs, J. W. DeCew, N.S Cohen and Van der Hoven, Blaauw, Pieters and Warnier regarding the concepts of privacy and surveillance.

3. STATE OF THE QUIESTION

The study and analysis of the relationship between moral convictions or morality and politics has been a recurrent theme throughout history. Interest in the relationship between these two subjects stems not only from the desire for greater knowledge of the human being, but also from curiosity about new techniques of political recruitment and manipulation in the electoral communication field. These techniques of political engagement have seen an increase with the surge and development of new technologies such as Social Networking Sites (SNS), also known as Social Media Platforms. This increase has its roots in the rise of the data available for political targeting, and that can be purchased from these platforms.

The purpose and reasoning on the use of this type of information and why new technologies have had such an impact on these political techniques, will be explained in the present chapter. To do this, the main theories concerning the study of moral values in relation to politics, and the concepts related to the use of data for political gain through and thanks to social media, will be presented below.

3.1.   <u>Moral convictions and politics.</u>

Moral convictions have been studied throughout history from many different fields of knowledge such as philosophy, psychology, or political studies. We have always tried to decipher the connexions between our deeper convictions and our behaviour. Through these studies we have come to the conclusion that there are in fact some ties or links between what we believe in or believe to be right, and how we act. These conclusions have also been extrapolated to explain political behaviour.

Linda J. Skitka Ph.D. Professor of Psychology at the University of Illinois studied these connexions in a research paper called "The Psychology of Moral Conviction". In the study, she explains why, when people have moral convictions with regards a certain topic, they tend to discriminate other people's beliefs if they are not similar. The deeper the moral conviction is, the harder it is for them to tolerate different opinions or

approaches towards the topic in question. These convictions are shown to be also important regarding people's perceptions of what is fair and what is not (Skitka, 2010).

This author also illustrates the impact moral convictions have in group behaviour. She shows, on the one hand, that people tend to agree with the group majority, in most of the times, because of rejection concerns and that this group pressure effect is highly effective when people do not hold an opinion with regards the topic that is being debated. On the other hand, people with strong moral convictions do not succumb to peer pressure and maintain their convictions while rejecting, as explained above, anything that is different from their beliefs (Skitka, 2010).

These conclusions can be applied to political behaviour as well. The association with certain moral convictions and political or voting behaviour has long been established. Because of what has already been explained, people with strong beliefs tend to see political parties aligning with those beliefs as the one that is fair, that is right and that therefore should represent them. Both the intolerance people with strong moral convictions develop towards ideas or political ideologies and agendas contrary to their core values, and the acceptance with regards those who share their moral principles, create a powerful emotional response (negative or positive) which later translates into voting behaviour. These psychological and behavioural practices have been seen both in the right and left of the political spectrum.

The idea that both sides of the political spectrum can see their political behaviour driven by certain moral principles, leads us to the conclusion that there are certain moral values aligned with either conservatives or progressists. This idea has been developed extensively by the American philosopher and cognitive linguist, George Lakoff. In his book *Moral Politics. How liberals and conservatives think,* he explains how conservatives tend to have a moral framework related to a more "strict father family values' approach". On the other hand, progressists have moral convictions similar to "nurturant parent family values" (Lakoff, 2010). As explained before, these different moral frameworks create a divide between political ideologies that is reinforced as the convictions become stronger. This is due to the increasing rejection of different moral frameworks to the ones held by each one of us. Because of the clear division and

differences between the two moral frameworks, it is therefore easier to make predictions about voting behaviour by looking at the voters' lifestyles, friends, families, education… This, consequently, means that new technologies have become an essential tool in the collection of this type of data not only for commercial but also for political purposes.

3.2. <u>Data mining and the commodification of data.</u>

Because of the importance of voting behavioural predictions, and knowing moral convictions play such an important role in them, data from Social Networking Sites has become one of the most valuable assets in global markets nowadays. The interest in knowing as much as possible about every user of each platform, either for commercial or political purposes has increased enormously. This collection of data, from our interactions and movements on the internet, can be beneficial in certain ways but has meanwhile developed many ethical concerns regarding both the collection and sharing of this data, and the use third parties make of it. For this reason, two important concepts related to data, which will serve as a basis for understanding the main analysis in this study will be presented below:

The first concept is the concept of "data mining". This concept has been defined by the Spanish energy company, Iberdrola, as:

> A technical, automated or semi-automated process that analyses large amounts of scattered information to make sense of it and turn it into knowledge. It looks for anomalies, patterns, or correlations among millions of records to predict outcomes (Iberdrola, 2021).

The company also explains the functioning of such techniques and that they are used:

> To explore increasingly large databases and improve market segmentation. By analysing the relationships between parameters such as customer age, gender, tastes, etc., it is possible to guess their behaviour in order to target personalised customer loyalty or recruitment campaigns (Iberdrola, 2021).

With this definition, we can see how this technique can be regarded as a really useful tool for political targeting during elections or other democratic processes such as referendums.

The second concept is "commodification of data". This concept can be defined as the capitalisation or value creation from the information provided by users or participants in Social Networking Sites. Although the information or content created is done so by the users, the profit is for the private companies owning these sites. So, as Nicole S. Cohen explains it: "as we spend time online, we generate information that is instantly collected, analysed, sold, and then presented back to us in the form of targeted advertisements that reflect our online behaviour and consumption patterns" (Cohen, 2013).

4. THEORETICAL FRAMEWORK.

Having introduced the main concepts and theories essential with regards the topic of this study (the use and abuse of data for electoral purposes), in the present chapter a contextualisation of the core aspects of the study will be made. To do so, it will be firstly explained the concept of privacy and its drift towards a surveillance situation; secondly, it will be explained what Brexit is, its historical context and why it happened, and why the Brexit referendum is an event that can be utilized as an example to show how data is used in political campaigning; finally, there will be a description and introduction of the main actors regarding what is known as and what will be our case study: "the Cambridge Analytica scandal".

4.1.   Privacy and Surveillance.

These two concepts or ideas, privacy and surveillance, are essential to the understanding of the present study. The reason of them being of such importance is, as will later be demonstrated, that they constitute the basis of the main ethical concerns that arise when studying the practices of several actors with reference to the use of data in political campaigning.

The first concept, privacy, has been defined by the Cambridge Dictionary as "someone's right to keep their personal matters and relationships secret" (Cambridge Dictionary, 2021). The same dictionary states that the meaning of this word in a business context would be "the right that someone has to keep their personal life or personal information

secret or known only to a small group of people" (Cambridge Dictionary, 2021). However, although these definitions can seem clear and representative of the concept, there have been and continue to be many discussions of weather this concept should be considered just a moral value, or if it should be granted a "human right" or "legal right" status. Nevertheless, despite the disagreements towards the term, all theorists seem to agree in the importance of it for human lives.

There are, apart from these aspects, other differences with regards the approach and the description of what privacy is. The highly awarded Professor, Judith Wagner DeCew, differentiates between two types of privacy. The first one is known as "constitutional privacy" and it refers to the freedom people have to make their own choices regarding issues that have to do with their personal and private lives. The second type, which will be the one used in this study, is "informational privacy", and it refers to individuals' interest in having control over the access others could have to information about themselves (DeCew, 1997). The latter would also imply the moral right people have to control new technologies that could be used or intended for creating, gathering, processing, or sharing this information. This is a very important aspect of the analysis that will be conducted later in this study. On the other hand, another important aspect is the interconnection privacy has with other important values such as liberty, dignity, intimacy or democracy, and that could see themselves undermined if the value or moral right of privacy is not protected as we will see later on in the study.

Having seen all these definitions and descriptions of what privacy is, we must make one final clarification before continuing with the reasons why it should be protected. This clarification refers to the distinction there is between a United States of America's terminology and a European terminology regarding the protection of privacy. The first one refers to the concept of "informational privacy protection" as "privacy protection", while the second one, which will be employed in this study, refers to it as "data protection". The reason for using this term (data protection) in the present study surges from its accuracy in designating the protection needed in the technological world in which the case study, that will be later presented, takes place.

Then, why is it important to have such protection of data or of privacy? As it has already been addressed, the moral value of privacy is intrinsically connected with other human essential values or rights, therefore the deprivation or deterioration in the protection of the first one can directly result in the worsening of the latter. The lack of privacy can thus derive in multiple moral dilemmas. Firstly, we find the degradation of an individual's human dignity that arises when, because of the lack of privacy and the ability of external actors to access one's personal information, the concerned individual sees its decisions influenced unconsciously, resulting in choices that without that interference the individual would not have made (Van der Hoven, Blaauw, Pieters, & Warnier, 2014). Methods as the already explained "data mining" and "commodification of data", along targeted advertising are among the main problems new technologies have generated, regarding privacy, over the past decades. Because of the novel nature of this technologies, the privacy protection mechanisms available until recently have been found not to represent the needs of this new technological era, and therefore have resulted in major breaches of privacy that some have defined as mass surveillance.

The author Christian Fuchs has defined this idea of surveillance as something that:

> Tries to bring about or prevent certain behaviours of groups or individuals by gathering, storing, processing, diffusing, assessing and using data about humans so that potential or actual physical, ideological or structural violence can be directed against humans in order to influence their behaviour (Fuchs, 2014).

This study will address the use of this type of surveillance implemented by different actors in political campaigns such as the one in the case study, the Brexit referendum. Because of this surveillance practices, and as we have explained before, personal information has become a commodity, but one that is not governed by an egalitarian contractual relationship, but by an unequal one, in which the individual, for the most part, does not have the possibility to decide how his or her data is accessed and under which conditions. This creates another moral conflict for which the only solution is a better understanding of the way in which these mechanisms work, therefore making it possible to create the necessary data protection structures or laws that prevent these

breaches and violations of values such as democracy, autonomy or security (Van der Hoven, Blaauw, Pieters, & Warnier, 2014).

Once it has been clarified what privacy is, and the moral reasons wherefore it must be protected against practices such as surveillance, it will now be addressed the impact new technologies, or more specifically information technologies, have had in this moral value. New technologies have increased the amount of information that is available worldwide, it has made possible to connect people from different corners of the globe at a speed that would have been unthinkable a few decades ago. But despite these positive developments, which have made people's lives so much easier, new technologies have brought with them new challenges and problems such as the one addressed in this study. The speed and ease of access to information has meant that, in some cases, this (often private) data has been abused resulting in mass surveillance, manipulation and even extortion thanks to these new technologies and ways of communication.

Some of these abuses have taken place firstly, on the internet, through the use of what is generally known as "Cookies". These ones are text files with small pieces of data that web sites store in one's computer. They were created with the aim of offering the user a more personalised experience online. The computer would remember what the latter's searches and websites were more recurrent, therefore presenting the user information that, according to the profile created by the computer of him or her through the cookies, could be more relevant. The problem with these so-called cookies is that the tracking of the user's history on the internet is often used, not only by the search engine or platform, but by advertising companies that could present the user with advertisings and publicity in a more recurrent way (adding the advertising in all the webpages that the person visits the most), and in a more persuasive way, given the ability of the data to show a profile of the user's tastes. This possibility cookies give to advertising companies can be regarded in two ways. It could be seen as beneficial in an economic sense because it allows advertisings to be more effective, but it could also be seen as detrimental to people's privacy and their capacity to make their own decisions

without an unknown interference or manipulation (Van der Hoven, Blaauw, Pieters, & Warnier, 2014).

Furthermore, the information and data available online have increased even more with the emergence of social media. Social networks, by design, invite users to share as much information as possible, the more the better, indicating percentages of improvement of a profile if more data is added. This feature, coupled with the existence of greater "peer pressure", as each user's data is made public to those with access to their profile, creates a greater privacy dilemma and another opportunity for data to be used for immoral purposes and manipulation. Moreover, the data available in social networks can be considered the best source of information for big data processing techniques such as "profiling" or the already defined "data mining" (Van der Hoven, Blaauw, Pieters, & Warnier, 2014). These techniques, as explained in the previous chapter, can result in the radicalisation of, not only people's tastes, but ideas (political, cultural, religious) and could be then externalise into these users' societies.

The above presented information about privacy, its risks, and the moral dilemmas that surround the term will be essential in the analysis of the case study and the practices that have been lately implemented in the digital sphere of political campaigns and other democratic processes like referendums. The key theoretical terms and actors necessary to contextualise the case study "The Brexit referendum and the Cambridge Analytica Scandal", will be dealt with hereafter.

4.2.   <u>What is the Brexit referendum?</u>

In order to understand the historical, political and social context of the case study that will be later analysed, it is necessary to look at the causes and consequences of the so-called "Brexit referendum" (because of the word combination of Britain and Exit). This referendum took place on the 23rd of June 2016 and marked the end of the United Kingdom's membership to the European Union project.

To understand why the United Kingdom decided to hold a referendum on leaving the European Union, we must go back in the country's history to 1973. In that year, the United Kingdom joined what was then known as the European Economic Community,

which years later would become today's European Union. The country, from its inclusion in the EEC, was marked by disparity of opinion regarding membership of this international organisation. Only two years after joining the EEC, in 1975, the first referendum on continued membership was held. On this occasion, unlike the 2016 referendum, the main opponents of remaining part of the (at that time purely economic) European project were left-wing parties such as the Labour Party. On the other hand, conservatives, led at the time by Margaret Thatcher called for a major voting turnout in order to remain in the European Economic Community (BBC, 2020).

The situation changed some years later with the signing of the Maastricht Treaty. This treaty transformed the hitherto economic union into a political union. Those who until then had decided to defend the European project began to express sceptical opinions about the new turn, and we can say that they gave rise to what we know today as Eurosceptics. The roles were reversed and the parties that advocated a No vote in the 1975 referendum now advocated the opposite. The same but in reverse happened with the Conservatives, in the previous democratic exercise they called for a Yes, and since that moment they gradually increased their criticism until the 2016 referendum. (Kirby, 2020).

Since then, the negativist discourse on EU membership has been growing and fuelling the mood of the Eurosceptic parts of the population. Despite this negative discourse, the UK has always enjoyed a position of power that gave it special and privileged conditions. Some of these privileges are, for example, the possibility for "opting out" of the acquisition of the single currency, the euro; not accepting the agreement establishing the Schengen area; not applying the EU Charter of Fundamental Rights in its territory; or, on the other hand, not being part of one of the most recent treaties, the Treaty on Stability, Coordination and Governance, which was rejected due to an agreement reached by the British Parliament under which no new cessions of sovereignty or competences to the EU should be approved during the term of that legislature (Mangas Martín, 2016).

Therefore, if the situation and status of the United Kingdom within the European institutions was different, why did a referendum take place? There are several reasons

why the UK became increasingly closer to Brexit, and which are of great relevance to understanding, later in this study, the techniques and messages used in the political campaign around the referendum. Firstly, there was a widespread fear, as discussed above, of a greater and closer political union, which would imply a further transfer of powers, and which was presented to the British citizens as a loss of national sovereignty. Another reason was the growing internal rift within the Conservative party, between those who advocated remaining in the EU and those who supported a citizens' consultation to push for an exit.

On the other hand, the economic and financial crisis of 2008 had a major influence. The consequences of the crisis, as in the rest of Europe, led to a rise of Eurosceptic and populist parties, something that also happened in this country with the growth of the extreme right-wing and highly anti-European UKIP party. A further argument for holding the referendum and leaving the European Union was the rejection by the so-called "City" of London (the country's financial centre) of the European Union's proposals for economic convergence, which they saw as a loss of autonomy and which were perceived as an injustice to those countries that did not have the common currency, the euro.

Finally, another argument, and probably the most used in the campaign, was border control. As a member of the European Union, the UK was obliged to comply with the principle of equality of all European citizens, which with the large-scale entry in 2004 of Eastern European countries, generally with lower purchasing power, led to large migratory movements from these countries to more economically prosperous ones such as the UK (Hutton, 2020). The problem with this argument is that it does not take into account the Directive 2004/38, which states that European citizens in other Member States cannot receive state aid and subsidies if they are unemployed for a maximum of three months, a measure intended to alleviate the "excessive" burden in the face of what has happened in countries such as the United Kingdom (Mangas Martín, 2016). This is important because, as will be seen below, the excessive burden of this opening of borders to European citizens was one of the main points of the campaign to gather votes in favour of leaving the European Union.

All these factors, in addition to the UK's historically turbulent relationship with the European Union, created the perfect context for David Cameron (a supporter of remaining in the European project) to promise a referendum in the election campaign if he was finally elected. Cameron won the election in 2014, becoming prime minister and holding the promised referendum two years later.
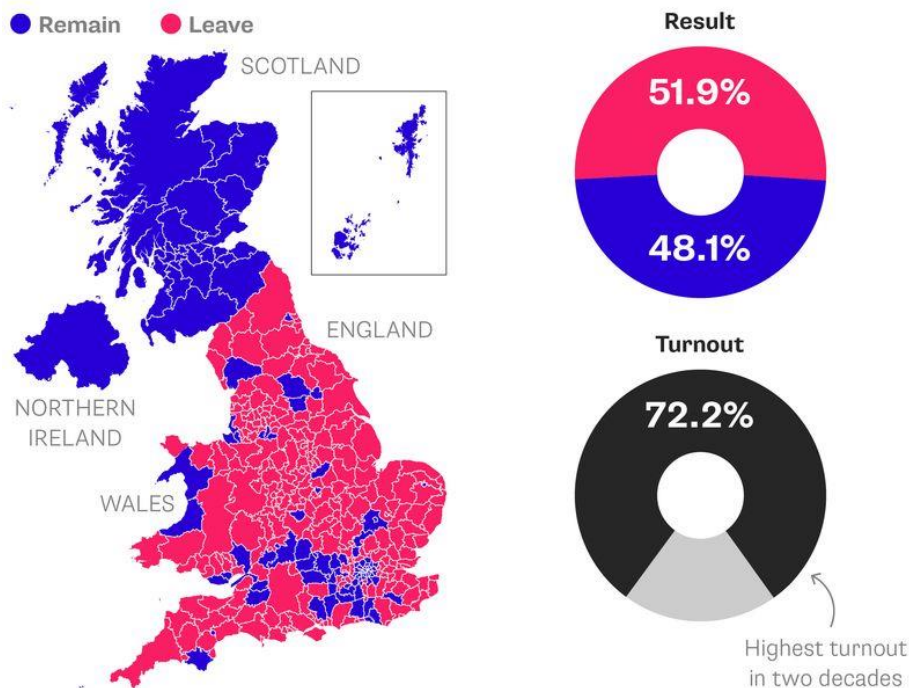

Figure 1. Source: (Hutton, 2020)

The result of the referendum was very close, as can be seen in *Figure 1*, but it marked the beginning of the UK's exit from the European Union and the resignation of Cameron, after he failed to get a majority vote to remain. The referendum was, however, fraught with controversy because of the practices used by both sides, especially the disinformation campaigns of the pro-exit campaign, and the use of data of thousands of Facebook users without their consent to achieve this result. It also plunged the country into political chaos until 2020 with the final exit from the EU, after four years of negotiations, three Prime Ministers and a surge in Scottish nationalism.

4.3.   Main actors of the case study.

In order to further understand the case study, which was given the name Cambridge Analytica Scandal, it is necessary to introduce the main companies involved in the case. This scandal was triggered by the discovery made by journalists from the New York Times, and The Guardian, and its magazine The Observer, about the illicit gathering and use of personal data of Facebook users and, therefore, of voters, for the manipulation of the latter through advertising campaigns carried out on the social network itself. The companies that had the most important role in the scandal, and which will be latter further analysed, were the following (House of Commons. Digital, Culture, Media and Sport Committee, 2018):

FACEBOOK.

Facebook is a social networking service that was launched in 2004 and that accounts for more than 2.85 billion active users which makes it one of the most remarkable and important ones in this sector. The company has been involved in many scandals regarding violations of privacy and political manipulation, being one of the cases the one that will be addressed as the case study. The reason why Facebook continues to be part of these scandals is that, as a capitalist company in search for profit, it has created an economic model in which targeted advertising is its major source of revenue. This means that the information or data shared by Facebook's users on the platform ends up being commodified and sold to advertising companies. The social network is not only the source of the information, but also the showcase in which these companies display their advertisements once they have been personalised and targeted (Fuchs, 2014).

SCL GROUP

SCL Group, which stands for Strategic Communication Laboratories, was a strategic communications company used, among others, by the United States of America's government as well as the British governments during the Afghanistan and Iraq wars, and which worked targeting elections mostly in developing countries (Barry, 2018). The company was originally oriented towards the intervention of election campaigns with

the aim of combating terrorist organisations, and the disruption of enemy intelligence in conflict areas. The company's economic model was based on data mining and data analysis with the aim of influencing electoral behaviour through advertisings in social networks and other digital platforms. The company closed operations in 2018 after the Cambridge Analytica Scandal.

CAMBRIDGE ANALYTICA LTD (CA).

Cambridge Analytica Ltd. was a company created in 2012 that described itself as a political consultancy firm operating in countries such as the United States of America. The company received its funding from Robert Mercer, also the largest donor to the US Political Action Committee (PAC) in support of politicians such as Donald Trump or Ted Cruz. Moreover, the company's Vice President was also Donald Trump's former White House chief Strategist, Steve Bannon. The company has been proved to be a subsidiary of the already existing and above mentioned, SCL Group, a company that used military techniques for the gathering and processing of data with the aim of manipulating political behaviour. Cambridge Analytica also gave the name to one of the biggest political and privacy scandals over the last decades (House of Commons. Digital, Culture, Media and Sport Committee, 2018).

AGGREGATEIQ (AIQ)

AggregateIQ is a Canadian technology and political consultancy company who also had an economic model based on data mining and data analysis for targeted advertising in political campaigns. The company worked among other democratic processes, in the campaign for leaving the EU during the Brexit referendum and was later the first company accused of breaking the GDPR, which is the European General Data Protection Regulation (Baraniuk, 2018). This company also collaborated in the development of the software tool that would be used by this company and Cambridge Analytica (and therefore SCL) in their different campaigns since 2014. This tool was in charge of creating the algorithms that would segment Facebook users according to their data, in order to subsequently carry out the placement of targeted ads at the social network and in other websites over the internet (House of Commons. Digital, Culture, Media and Sport Committee, 2018).

5. CASE STUDY ANALYSIS.

As indicated above, this thesis will analyse the case of the scandal known as the Cambridge Analytica scandal. Due to the scale of this affair, this thesis will limit the scope of the study to the impact of this particular case on the Brexit referendum, which context was explained in more detail above. Before conducting the mentioned case analysis, we need to firstly understand how the scandal became a matter of interest and investigation.

Carol Cadwalladr, one of the journalists who investigated and uncovered the case, started the investigation in 2017 because she could not understand why in places like Ebbw Vale, a small town in Wales, where immigration was practically non-existent and where European infrastructure funding was highly visible, the inhabitants argued in favour of the UK's exit from the European Union by claiming to be tired of immigration and saying the EU had done nothing for them. Cadwalladr began to investigate the source of the information received by these people and after interviewing several of them concluded that this information came from advertisements seen on the social network Facebook. In addition, she began looking for information about a company called Cambridge Analytica that, according to her investigation, had links to Trump's 2016 election campaign and the Brexit referendum campaign that same year. Through her research she discovered that this company, as we have already explained, was a company dedicated to the creation of political profiles of users through their data, subsequently helping in the targeting of advertisements to them, thus benefiting the effectiveness of the advertising campaigns or in this case political campaigns, of its clients. Carole Cadwalladr also discovered that the data used by this company had been obtained illegally and without the knowledge of the owners of this data (around 87 million Facebook users), making it therefore a case of covert electoral manipulation and privacy breaching produced entirely on Facebook (Kang & Frenkel, 2018). All this information about the scandal was obtained by the journalist thanks to the former employee and co-founder of Cambridge Analytica, Christopher Wylie, who acted as a whistle-blower and uncovered the practices used by this company and other similar companies in the referendum campaign, and in other democratic processes such as the

aforementioned US presidential campaign in 2016 or others in countries such as Trinidad and Tobago or Nigeria (Cadwalladr, 2019).

To better understand the case, we will now explain the relationship between these companies and the Brexit referendum chosen for study. We will then analyse the methods and techniques used by these companies and some advertising examples employed during the campaign. Finally, it will be considered the impact these techniques could have in the result of the referendum.

5.1. How are these companies related to the Brexit referendum campaign?

The link between the company that gives its name to the scandal, Cambridge Analytica, and the Brexit referendum has turned out, after the British government's own investigations through a commission of enquiry, not to be as easy to prove as it might have seemed at the beginning of the investigations. This is because several pro-Brexit
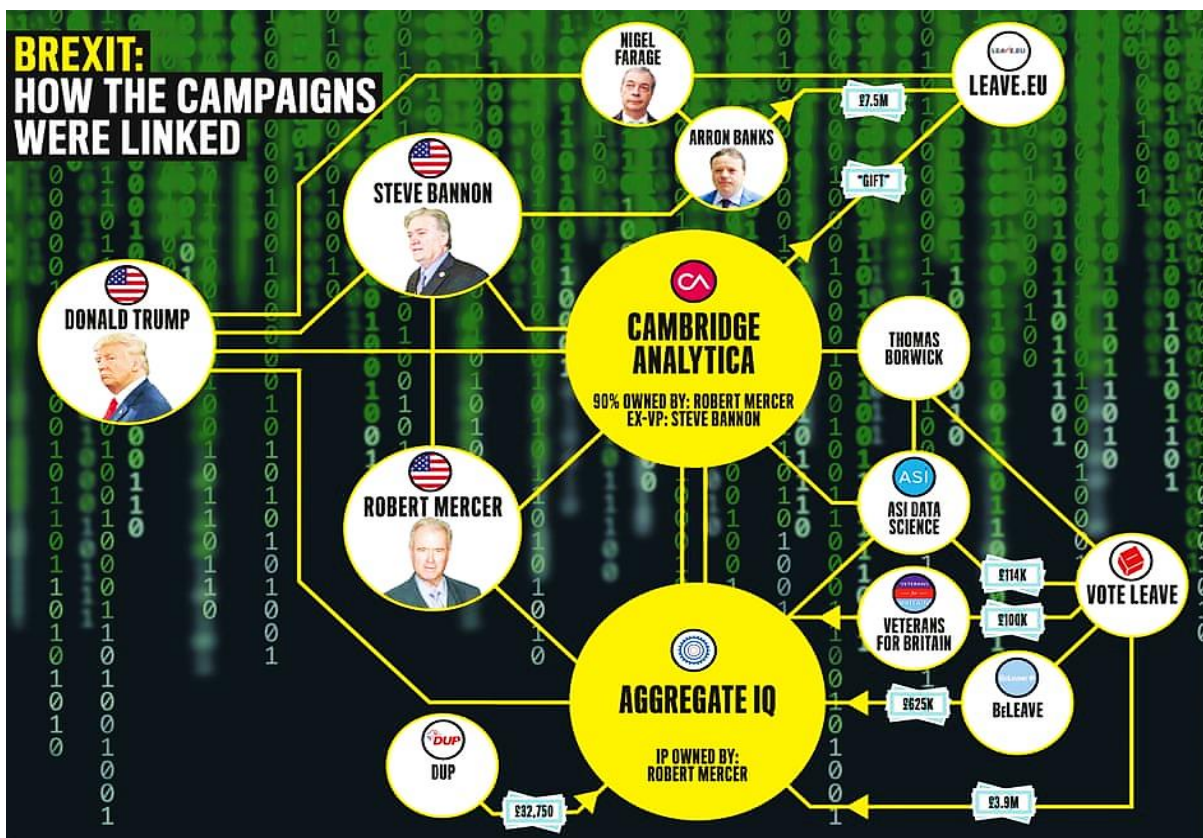
Figure 2. Explanatory image of the links of the Brexit referendum campaign actors.
Source: (Cadwalladr, 2017)

campaigns, external actors, as well as companies similar to the one mentioned above, are involved in the investigation, making it difficult to establish direct and causal links

regarding the scandal. Therefore, in order to facilitate the understanding of the case, we will use the explanatory image below (Figure 2) and the findings of the UK's Information Commissioner's Office (ICO).

In order to understand how the scandal of analysis unfolded, it is necessary to identify the main (electorally recognised) groups that participated in the campaign advocating a vote in favour of the UK's exit from the EU. The first of these groups, though not considered the official campaign, was Leave.EU. This group was founded by British businessman Arron Banks, also a major donor to the UKIP party, to represent British Eurosceptics. The group was later recognised by UKIP leader Nigel Farage as the main campaign, although the latter later clarified that he supported all pro-leave campaigns as they targeted different population groups (Wylie, 2019). The Leave.EU campaign was focused on and represented the far-right wing of British politics, loaded with anti-immigration messages, as we will see in more detail later in this chapter.

On the other hand, there was the Vote Leave campaign. This group was mainly composed of members of the Conservative party, i.e. mainly members of the Tories who, unlike David Cameron, were in favour of the UK's exit from the EU. The main political faces of the campaign were the current British Prime Minister, Boris Johnson, and another British Conservative MP, Michael Gove. The group was co-founded in 2015 by the conservative political strategist Dominic Cummings and the founder of several British conservative lobby groups, Matthew Elliott.

Cambridge Analytica's whistle-blower, Christopher Wylie said, in his statements to the Information Commissioner's Office's investigation and in his book about Dominic Cummings and another of Vote Leave's political strategists, Stephen Parkinson (at the time former special adviser to then Home Secretary Theresa May), that they:

> Knew that they weren't going to win the vote by speaking only to traditional right-wing Brexiteers, so Vote Leave made it a priority to bring in a more diverse coalition of support. In British politics, referendum campaigns are unique in that they tend to make a concerted effort to be as cross-party as possible, because issues, not parties, are on the ballot. No one "wins power" at the end of a referendum; only the idea wins, and the government of the day has a choice

whether or not to implement the result. Cummings and Parkinson understood
that the key to a Brexit victory was to identify Labour and Lib Dem voters, as well
as those who didn't normally vote, and persuade them to either vote Leave or
stay neutral (Wylie, 2019).

Because of this approach, the Vote Leave group decided to partner with another pro-
leave group aimed at this younger and progressive audience, with which they could
complete the ideological spectrum in an effort to reach the maximum amount possible
of citizens and convince them to vote in favour of a "Brexit". This mainly financial
"alliance" has turned out to be illegal, according to investigations conducted by the
British Electoral Commission, taking into account that by associating, both groups would
have incurred an overspending in campaign advertising, exceeding the limits allowed by
law in the United Kingdom.

Once we are familiar with all the main groups involved in the pro-Brexit campaign, which
were also involved in the scandal analysed in this study, we can proceed to explain the
relationship between Cambridge Analytica and the referendum process in the UK, and
how it exposed multiple problems with regard to the use of data in political campaigns.
To do so, we will begin with the Leave.EU campaign during the referendum. In
November 2015, prior to the vote, a team from Cambridge Analytica, including Brittany
Kaiser (who would later become another whistle-blower speaking about her work at the
company), visited Leave.EU's headquarters. These were located in Bristol, within the
offices of Eldon Insurance (Arron Banks' insurance company) and occupied by the
company's workers who appeared to be working on the campaign as well. Cambridge
Analytica had made the visit as Leave.EU and the company were doing preliminary
consultancy work, with which CA intended to show how it could help the campaign.
Following the visit, Cambridge Analytica offered its services and asked for all the data
held by Leave.EU to be transferred to begin the analysis of the data, which would be
phase 2 of the process. The data was sent to the consultancy firm, analysed and
discussed with the group, although the documents containing the official analysis were
not delivered. After this period of analysis, and calls about what was being found, the
relationship between CA and Leave.EU ended, and as Brittany Kaiser herself indicates in
her book *Targeted*:

The apparent end of our working relationship with Leave.EU left us in a confusing place. After all, we'd been publicly associated with them since November. In all, we'd spent three days consulting with them, two in preparation for the press conference, and one in Bristol, trying to get their team up to speed. This was in addition to the many man hours we'd spent working with the data they'd given us, to complete phase one and prepare for the news conference presentation. We'd never given them the slides, but I had talked through the findings in the slides in great detail with the Leave.EU team over the course of those days. Yet, for all that work, we never received a signed contract or payment, which made it hard for us to take credit for the work or move forward (Kaiser, 2019).

Following the end of the business relationship, the Leave.EU campaign continued successfully. It focused on campaign ads (many of them on Facebook) that were mainly about immigration. We will analyse one of the ads below. However, Kaiser herself indicates in her book that she finds it hard to believe that a campaign so similar to what they had discussed during their consultations could have taken place without the Leave.EU team making use of the targeting insights.

Another problem that arose from this campaign, the Leave.EU campaign, is the collection and use of data belonging to Arron Banks' companies (e.g., Eldon Insurance), and its subsequent use for purposes not known by the data owners, such as targeted advertising. The report that investigated this issue stated that "more than a million emails sent to Leave.EU subscribers contained marketing for the Eldon Insurance firm's GoSkippy services", and that Leave.EU was also "using Eldon Insurance customers' details unlawfully to send almost 300,000 political marketing messages" (BBC, 2019)

On the other hand, the group Vote Leave, created in 2015 by Dominic Cummings, partnered with the company AggregateIQ during his campaign. This company, dedicated as explained above to data mining and the development of targeted advertising, was responsible for developing the algorithms and processing the data of British voters to subsequently use the profiling of the same to display ads favourable to Brexit and personalised according to their interests. As Brittany Kaiser explains in her book about the Scandal:

The strategy used focus groups, psychographic modelling, and predictive algorithms, and it harvested private user data through online quizzes and contests, using a perfectly legal opt-in. For Brexit, the campaign had matched user data to British voter logs and then it injected itself into the bloodstream of the internet, using targeted messaging to incite a nation (Kaiser, 2019).

As Kaiser explains, Vote Leave conducted big data harvests through subscribers' details available to the group, from other voters from whom registration data could be obtained, and finally through online surveys and competitions. This is the case of the contest launched by Vote Leave which offered the chance to enter a competition to win £50 million by guessing the result of all 51 matches of the European Football Champions League (almost an impossible task). This competition, which was called "50million_remains" and was advertised in Facebook as seen in *Figure 3*, aimed to collect data such as the name, address, email, telephone number and voting intention of anyone who wanted to participate (Cadwalladr, 2018). All of this data was then analysed by Aggregate IQ through machine learning and

Figure 3. Advertising from Vote Leave for the Brexit Campaign. Source: (BBC , 2018).

matched to the data that Facebook employs about its users for its digital advertising platform to deliver targeted advertisings (McGaughey, 2019). With this technique, as Christopher Wylie indicates in his book:

More than a hundred different ads with 1,433 different messages to their target voters in the weeks leading up to the referendum. Cummings later revealed that these ads were viewed more than 169 million times, but only targeted at a narrow segment of a few million voters, which resulted in their newsfeeds being dominated by Vote Leave messaging (Wylie, 2019).

Following the referendum and the research carried out by the Information Commissioner's Office, it was found that AIQ had failed to comply with the GDPR as:

(1) AIQ failed to comply with article 5(1)(a)-(c) and article 6 GDPR by processing "personal data in a way data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing". In addition, the "processing was incompatible with the purposes for which the data was originally collected". (2) AIQ failed to comply with articles 14(1) and (2), as it did not provide data subjects with the required information regarding the processing of their data, in circumstances where the data was not obtained from those data subjects (Stevens & Bolton, 2019).

With this, and as it has been already mentioned, Aggregate IQ became the first company to receive a formal notice from the ICO regarding the breaching of the European Union's General Data Protection Regulation (GDPR) (Baraniuk, 2018). The successive investigations that have taken place into this scandal have also concluded that, although AIQ was closely linked to the communications consultancy Cambridge Analytica and therefore to its parent company SCL Group, there is no evidence that they were linked during and in relation to the Brexit referendum (Denham , 2020). This would imply that despite the preliminary work carried out by CA for the Leave.EU team, the company was not formally involved in the campaign to leave the UK as far as is known to date. Therefore, although the company gives its name to the data use scandal surrounding the 2016 UK referendum, it has not been proven that it was involved in the latter. Nevertheless, the company did participate in other campaigns, such as that of Donald Trump in 2016, using techniques similar to those we will see below, which were used during the campaign by pro-Brexit groups.

5.2. Analysis of the used techniques and advertising for the Brexit referendum campaign.

Companies such as the aforementioned Cambridge Analytica, SCL or AggregateIQ work with the same techniques of persuasion through the analysis of personal data for the subsequent personalisation of advertising. We will now try to explain how these companies work and we will examine some of the advertisements published by them during the course of the referendum campaign.

With the development of new technologies such as social networks, companies dedicated to communication and advertising consultancy during electoral campaigns or other democratic processes have made a change of strategy that allows them to take advantage and adapt to the benefits of these new developments. Social media allows political campaign messages to have much more impact and reach people who are more difficult to interact with. In addition, they allow the message to appeal to a greater extent to the interests of the audiences and thus achieve a higher response rate, which translates into an increase in the effectiveness of the campaigns. Companies such as those mentioned above, and others like them that still exist today, decided to take advantage of such benefits through deep data analysis and targeted advertising.

The problem with these practices stems from the way in which the data is obtained, and the manipulation of the data for purposes outside the knowledge of the users and therefore the people to whom the information belongs. During the Brexit referendum these practices were used. The different pro-Brexit groups, thanks to companies such as CA or AIQ, started harvesting data through methods of dubious morality and even declared illegal. Some of these data collection processes are the previously mentioned contests initiated by Vote Leave, or the use of customer data from other companies, such as Eldon Insurance, by the Leave.EU group. Once the data has been collected, the electoral consultancy firms carry out analyses of the information by means of which they are able to create profiles of each of the people behind the data. Through these profiles, political groups can find out the person's geographical location, age, sex, interests and even political affinity. Once this data is identified, it will be easier to appeal to the interests of these people in order to persuade them to vote in favour of the ideology presented in the advertisement. This is achieved by placing the advertisements in the most frequented places of these individuals, their social networks and the websites most visited by them (Information Commissioner's Office, 2018). Following the analysis made above regarding the relationship of these companies (CA, SCL and AIQ) with the Brexit campaign, we know that each campaign, although advocating for the same objective, was aimed at a different audience. To show how each of them worked, we will show and discuss below some of the ads that were placed by each campaign group.

Firstly, we can find the campaign of Leave.EU. The latter, as we have indicated before, targeted an audience that was mainly ideologically from the far-right. Despite this segment of the audience, Arron Banks' campaign was also able to obtain the data of people with security concerns from his own insurance company, and thereby get their profiling on the internet to receive advertisements such as the one shown in *Figure 4*, which displays a highly anti-immigration message with allusions to insecurity.

Figure 4. Advertising from Leave.EU for the Brexit campaign. Source: (Cadwalladr, 2019)

On the other hand, we know that the Vote Leave campaign was also focused on showing its audience the migration problem of staying in the EU. However, this campaign also addressed economic issues such as the protection of the National Health System (NHS), which they claimed could be achieved with the elimination of EU funding as we can see in *Figure 5,* or the concerns related to the 2008 crisis and the Greek debt. These advertisements were aimed at older people that had been identified due to the different data gathering methods as was the £50 million competition (BBC , 2018).

Figure 5. Advertising from Vote Leave for the Brexit campaign. Source: (BBC , 2018)

Finally, as we have already explained, the Brexit campaign, being a referendum, had to appeal to all kinds of ideologies from all segments of the population. Therefore, BeLeave's campaign through AIQ also personalised ads that were aimed at a younger and more progressive audience. This is illustrated by Christopher Wylie in his book as follows:

BeLeave's graphics focused on progressive issues such as the "tampon tax," arguing that if Britons were out of the EU, they would not need twenty-seven other member states to agree to get rid of what was so obviously a misogynistic tax. It seemed that there was a clear market for BeLeave's progressive, woke, and social-justice-oriented brand of Euroskepticism (Wylie, 2019).

In addition to this example, other advertisements aimed at the younger population talked about youth rates of unemployment, comparing, as we can see in *Figure 6*, the EU countries with the highest unemployment percentage with the unemployment rate in the UK.
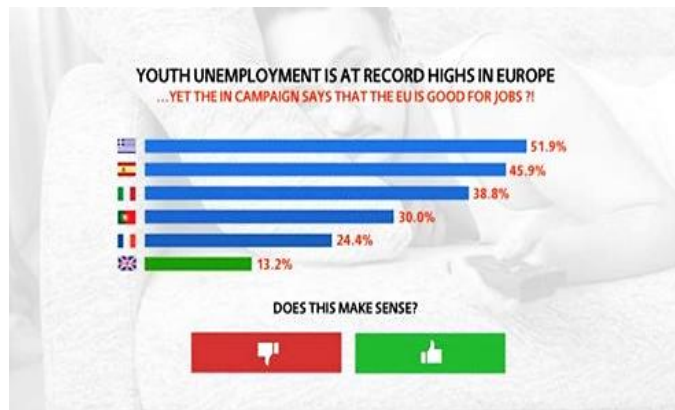
Figure 6. Advertising from BeLeave for the Brexit campaign. Source: (BBC , 2018)

Other ads were also aimed at people with a strong interest in animals. The advertisements targeted at these people showed, for example, the image of bullfighting events with a phrase "they are animals, not entertainment" as we can see in *Figure 7*. They tried to appeal to

Figure 7. Advertising from BeLeave for the Brexit campaign. Source: (BBC , 2018)

love for animals in relation to the EU's permissiveness towards such events.

All of these techniques used the generation of emotions such as fear or anger to produce a response from the audience. Thus, if an animal lover sees that the EU does not respect animal rights, or if a person concerned about security sees that their society is in danger according to the information that appears on their social networks, they will not only be willing, but will want to mobilise their vote to prevent it. This is why these persuasion

techniques are so effective, although they generate multiple moral conflicts around them, as we will see below.

5.3. Did these techniques have an impact on the Brexit referendum result?

Although we can be sure of the effectiveness of the microtargeting methods exemplified in this study, and we can see how companies and political parties around the world have increased their investment in these types of digital communication tools, it is impossible to know for sure the real impact they have. Therefore, as it has been concluded in the investigation conducted by the Information Commissioner's Office:

> It is impossible for us to say whether the data techniques used by either side in the UK EU referendum campaign impacted on the result. However, what is clear is that we are living in an era of closely fought elections, where the outcome is likely to be decided on the votes of a small number of people. There are significant gains to be made by parties and campaigns which are able to engage individual voters in the democratic debate and on areas of public policy that are likely to influence the outcome (Information Commissioner's Office, 2018).

As the investigation report states, although the influence of these data techniques on the outcome of the referendum cannot be established or proven, the referendum result was so close (only 1,269,501 votes of difference) that any kind of campaigning practice that could give an impulse to a campaign could have made a difference in the outcome. The problem with this is that, with new technologies, there is an increasing possibility of data being used for manipulative purposes, as it could have been in the referendum campaign for the UK's exit from the European Union.

6. ETHICAL CONTROVERSIES OF THE USE OF DATA MINING IN POLITICS.

As we have indicated over the course of this study, there are many ethical concerns that arise not only from the concerned case study, the Brexit referendum campaign, but also from the data and advertising techniques used in this case which could also be used in

the future.This is why we will now introduce these main moral concerns that arise from them and that have been studied by different scholars.

The main ethical problem is the one related to privacy. The techniques that have been already presented lead to practices that can be considered as surveillance-based techniques and with which every movement of a certain user of a platform is tracked and analysed to create a profile that can be then sold to advertising companies, political parties… With this profile of each user, the new owners of the data can more effectively predict their behaviour and bombard these people with targeted advertisings that will appeal to their deepest beliefs, interests and emotions, achieving in many cases an effective and desired response from the part of the user. The problems with this type of advertising is that the user in question lacks control over its own data, which can be used in ways not intended by the user when posting them in these platforms (Vallor, 2016) and which is being sold to third parties increasing the risk of misuse of that data and an even greater loss of control of the data in question.

Another ethical problem with regards these techniques is the use of algorithms during the process of data mining that tend to create "echo chambers" or "filter bubbles". The latter are filters created to present the user mainly with the information, advertisings, and other users' posts, that the concerned person is willing to like or agree with according to their profile (which in turn is based on that person's lifestyle, friends, searches on the internet, likes…). These practices can lead, as it was explained before with the link between intolerance and moral convictions, to the radicalisation of the user's ideas dealing the lack of confrontation of that person to different opinions or ideologies. Meanwhile, it can also result in the engagement of independent or indecisive voters, for example, by creating some kind of peer or group pressure appealing to the voter's principles, which will in turn result in the latter's engagement. This is because, as Ariel James argues there is an indivisible relation between morality and principles, emotions, and actions (James , 2017).

Therefore, if a political party creates certain advertisings aimed at attracting the indecisive voters, they will be more prone to like them if people they know liked them as well, which is something specifically and firstly shown in posts in the different Social

Media platforms (where the likes of the people you follow appear first), or if it reflects their moral values and principles (Bennett, 2012).

These procedures favour more radical and populist parties over the ones that follow a more moderate ideology. This is because of the attractiveness of the discourses of this first type of political party in terms of the creation of an emotional response and, as it has been explained, the algorithms these platforms use. The ethical risk of these methods, consequently, could be the undermining of democracy as a result of the loss of fair and ethical political campaigns.

A good example of these problems is the referendum campaign. This campaign shows how Facebook users who took the survey to participate in the £50 million competition, or customers of the Eldon Insurance company, lost control over their data and it was used for purposes beyond their knowledge and consent. The campaigns carried out by the different groups also demonstrate the link between moral principles and political action. This is because the techniques used show that a person concerned about security, in the presence of a possible threat to it (as indicated by the Vote Leave or Leave.EU ads in relation to immigration) will be more willing to act against the latter in this case, voting Leave. The same can be said of advertisements presented to people committed to animal welfare, gender equality or care for the elderly.

On the other hand, the communication during the referendum, and the creation of "echo chambers" with the bombardment of information about one of the voting options (centred on immigration) has led to a further radicalisation of the population resulting in an increase in racist crimes (BBC, 2019).

7. CONCLUSIONS.

Throughout the study, we have been able to analyse the impact of new technologies on today's political campaigns. We have been able to verify that they represent certain advances in terms of effectiveness in communication or in terms of interaction with the sectors of the population that are most difficult to reach, such as those who are not interested in politics or those who do not have a predefined idea about their vote. We

have seen how technology also helps in the processing of voter data which facilitates better tailoring of the advertising messages presented to voters, resulting in greater effectiveness. To this end, algorithms are based on ideas such as the one presented by Linda J. Sikitka, who argues for the link between people's morals and values and their political response or action.

However, the Cambridge Analytica scandal during the referendum on the United Kingdom's exit from the European Union has demonstrated the fragility of the system that allows this type of methods in campaigns, and the multiple dilemas or moral conflicts that arise from the use of personal data for the subsequent political manipulation of the owners of such information. It has become clear that not only are there serious threats to people's privacy on the internet, but there is also a grave danger lurking for democracy. This danger arises from the increasingly frequent manipulations, carried out by political parties or external actors, without people knowing that they are being subjected to such targeting. Societies such as the UK and the US have seen that the use of these practices in politics has led to an increase in the ideological radicalisation of the population, resulting in an increase in social polarisation and tension.

All these moral issues arise at the same time that companies like Cambridge Analytica, SCL or Aggregate IQ are profiting from this manipulation, and companies like Facebook continue to base their business model on facilitating it. This is why steps must be taken to regulate new technological developments, which are not reflected in electoral laws that were created long before they existed or were in place.

Nowadays, the Internet, and therefore the big companies that operate it, are based on the premise that, in order for your data not to be stored, analysed and sold to third parties, you must deliberately reject the terms and conditions of each of the websites that you visit on a daily basis. This means that the Internet does not defend people's moral rights to privacy but rather favours the lucrative right of those whose economic models are based on microtargeting. On the other hand, election laws do not address all these moral and ethical issues arising from the use and abuse of data for political purposes. For all this, the system must change and adapt to the new needs of privacy

protection, freedom of opinion without external influences, and finally, the possibility of confrontation of ideas which, because of these personalisation algorithms, are becoming less and less common.

To achieve this protection, the consent model for data collection and analysis should be completely contrary to the current model. This means that the user should have the option to share information, not the option to refuse to share it. Therefore, if the internet marketplace model were to be reverse-focused, it would be up to the user to decide what data they are interested in sharing, in an informed way, and not what data they do not want to share from a default list, meaning a change from an "opt-out" approach to an "opt-in"one. Electoral laws in turn should begin to contemplate that traditional, regulated forms of political campaigning are taking a back seat, and that digital communication is now indispensable. On this basis, the latter should be regulated to prevent not only manipulation or indoctrination, but also interference from external actors with geopolitical or commercial interests that have nothing to do with the society undergoing elections. This is because there are multiple companies similar to Cambridge Analytica, SCL or Aggregate IQ that continue to operate around the world.

All in all, we can conclude that there are multiple moral concerns arising from practices related to the use and abuse of data, most of which can be seen in the case of the so-called Cambridge Analytica scandal and Brexit, and that a system change is needed to regulate these practices in order to protect privacy, the right to decide of individuals and, with all this, democracy.

8. BIBLIOGRAPHY

Baraniuk, C. (2018, September 21). Vote Leave data firm hit with first ever GDPR notice. *BBC*.

Barry, E. (2018, April 20). Long Before Cambridge Analytica, a Belief in the 'Power of the Subliminal'. *New York Times*.

BBC . (2018, July 26). Vote Leave's targeted Brexit ads released by Facebook. *BBC News*.

BBC. (2019, June 20). Brexit 'major influence' in racism and hate crime rise. *BBC News*.

BBC. (2019, February 1). Brexit: Leave.EU and Arron Banks' firm fined £120,000 over data breaches. *BBC News*.

BBC. (2020, January 31). Brexit: A brief history of Britain and the EU. *BBC Newsround*.

Bennett, W. L. (2012). The personalization of politics: Political identity, social media, and changing patterns of participation. In W. L. Bennett, *The annals of the American academy of political and social science 644(1)* (pp. 20-39).

Cadwalladr, C. (2017, May 7). The great British Brexit robbery: how our democracy was hijacked. *The Guardian*.

Cadwalladr, C. (2018, May 20). Vote Leave faces scrutiny over £50m football contest. *The Guardian*.

Cadwalladr, C. (2019). Facebook's role in Brexit - and the threat to democracy. TED Talks.

Cambridge Dictionary. (2021). *Cambridge Advanced Learner's Dictionary & Thesaurus.* Cambridge University Press.

Cambridge Dictionary. (2021). *Cambridge Business English Dictionary .* Cambridge University Press.

Cohen, N. S. (2013). Commodifying Free Labor Online: Social Media, Audiences, and Advertising. In N. S. Cohen, *The Routledge companion to advertising and promotional culture* (pp. 177-191).

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics and the Rise of Technology.* New York: Cornell University Press.

Denham , E. (2020). Letter from the Information Commissioner . *ICO/O/ED/L/RTL/0181*, (pp. 1-18). London.

Fuchs, C. (2014). Facebook: a Surveillance Threat to Privacy? In C. Fuchs, *Social Media: A Critical Introduction* (pp. 153-178). London: SAGE Publications Ltd.

House of Commons. Digital, Culture, Media and Sport Committee. (2018). *Disinformation and "fake news": Interim Report. Fifth Report Session 2017-19.* London: House of Commons.

Hutton, R. (2020, February 1). The Roots of Brexit. *Bloomberg*.

Iberdrola. (2021, May 9). *Innovación.* Retrieved from Iberdrola Web site: https://www.iberdrola.com/innovacion/data-mining-definicion-ejemplos-y-aplicaciones

Information Commissioner's Office. (2018). *Investigation into the use of data analytics in political campaigns. A report to Parliament.* London.

James , A. (2017). The moral continuum: Congruence, consistency, and continuity in moral cognition. *Theory & Psychology, V. 27, 5*, 643-662.

Kaiser, B. (2019). Chapter 11. Brexit Brittany. Spring Summer 2016. In B. Kaiser, *Targeted. The Cambridge's Analystica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again.* (pp. 72-74). HarperCollins.

Kang, C., & Frenkel, S. (2018, April 4). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. *The New York Times*.

Kirby, J. (2020, January 31). A short history of the long road to Brexit. *Vox*.

Lakoff, G. (2010). *Moral Politics. How Liberals and Conservatives think.* University of Chicago Press.

Mangas Martín, A. (2016). La retirada del Reino Unido de la Unión Europea. *Foro. Revista de Ciencias Jurídicas y Sociales, Nueva época*, vol. 19, núm. 1.

McGaughey, E. (2019). Why we need a Democracy Protection Act before the general election. *London School of Economics - Brexit blog*.

Skitka, L. J. (2010). The psychology of moral conviction. In L. J. Skitka, *Social and Personality Psychology Compass 4 (4)* (pp. 267-281). Blackwell Publishing Ltd.

Stevens & Bolton. (2019, March 18). *Articles. First GDPR Enforcement Action is Against a Canadian Data Controller.* Retrieved from Stevens & Bolton: https://www.stevens-bolton.com/site/insights/articles/first-gdpr-enforcement-action-against-canadian-data-controller

Vallor, S. (2016). Social Networking and Ethics. In S. Vallor, *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University.

Van der Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2014). Privacy and Information Technology. In J. Van der Hoven, M. Blaauw, W. Pieters, & M. Warnier, *The Stanford Encyclopedia of Philosophy.* Metaphisics Research Lab, Stanford University.

Wylie, C. (2019). Chapter 9. Crimes Against Democracy. In C. Wylie, *Mindf*ck. Cambridge Analytica and the Plot to Break America.* (pp. 60-66). New York: Penguin Random House LLC.