ISSN (online): 2014-2242 / www.cac.cat

QUADERNS DEL CAC

Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016

Sara Suárez-Gonzalo
Predoctoral researcher in the Department of Communication at Pompeu Fabra University

sarapaz.suarez@upf.edu
ORCID Code: orcid.org/0000-0001-6883-1984.

Article received on 23/04/2018 and accepted on 11/07/2018

Abstract

The newspapers Observer *and* The New York Times *have revealed an alleged massive-scale scandal of data corruption involving Facebook and Cambridge Analytica that could have benefited the electoral victory of Donald Trump.*

The objective of this article is to analyze the conditions of possibility of the case and its potential influence on Americans' voting decision. To do so, it examines the scientific-technological, business and legal context related to big data technologies in which the facts would have happened and evaluates their possible influence in relation to the limits of the performed strategy and its current media and socio-political context.

Keywords

Big data, personal data protection, Donald Trump, Facebook, Cambridge Analytica, media manipulation.

Resum

Els diaris Observer *i* The New York Times *han revelat un suposat escàndol de corrupció de dades a escala massiva que involucra Facebook i Cambridge Analytica i que podria haver afavorit la victòria electoral de Donald Trump.*

L'objectiu d'aquest article és analitzar les condicions de possibilitat del cas i de la seva influència potencial en la decisió de vot nord-americà. Per a això s'examina el context cientificotecnològic, empresarial i legal relacionat amb les tecnologies big data en el qual s'haurien produït els fets, i es valora la seva possible influència en relació amb les limitacions pròpies de l'estratègia emprada i el seu context mediàtic i sociopolític actual.

Paraules clau

Big data*, protecció de dades personals, Donald Trump, Facebook, Cambridge Analytica, manipulació informativa.*

Introduction

On March 17, 2018, the newspapers *Observer* and *The New York Times* published the testimony of a new "whistleblower" named Christopher Wylie. The news reports revealed the supposed improper transfer of the data of millions of Facebook users to the company Cambridge Analytica, along with the fact that this company may have used these data to favour the victory of Donald Trump in the 2016 US general elections via a micro-targeting strategy based on military psychological attack techniques. It also reported that some of the data collected in the United Kingdom may have been used in the "Vote Leave" and "BeLeave" campaigns to push for the vote in favour of Brexit in the referendum held on the 23rd of June 2016.

Due in part to media leaks like this one, which is related to data corruption and the possibilities currently afforded by big data gathering and analytics technologies, citizen concern over the privacy of personal data has increased in recent years (Hargittai & Marwick 2016; Turow, Hennessy & Draper 2015). Despite the fact that big data analytics are still a more developed form of quantitative analysis, there are major new developments: data collection is indiscriminate and their processing draws from aggregation and cross-referencing techniques (Baruh & Popescu 2015) which enable information to be inferred from data even if it is not explicitly contained therein (Tufekci 2015). Different academic disciplines have made a decisive contribution to the technical development of the possibilities afforded by big data analytics and to reduce its costs. As a result, organisations and public and private institutions have already begun to use big data for different purposes. Market predictions, targeted advertising, improvements in the transport sector, the pursuit of terrorists, public health and the management of natural disasters are just several examples (European Parliament Resolution, 14 March 2017). However, beyond this, a business model has begun to gain ground that is based on data exploitation and dominated by large tech multinationals.

Big data technologies are not only increasingly complex, but they are also particularly opaque (Pasquale 2015), given that

there are major power interests at stake in data exploitation. For this reason, the 'notice and choice' model (Baruh & Popescu 2015) underlying Western data-protection laws is insufficient to deal with the social impact of big data phenomenon (Suárez-Gonzalo 2017).

Just like any technological advance, big data gathering and analysis methods and tools run the risk of falling into the wrong hands or being misused. The Cambridge Analytica case exemplifies this danger, but beyond that it also illustrates many of the risks entailed in the current development of big data. On the one hand, it reveals the threats that it poses to privacy and personal data protection, as well as the inadequacies of the current laws. On the other hand, it allows us to debate its influence on the rise in media manipulation, online disinformation and the radicalisation of ideas and political opinions (Marwick & Lewis 2017).

The aim of this article is to show that the seriousness of the Cambridge Analytica case is more closely associated with the existence of a structure that makes it possible and its social impact, as opposed to the possible specific interference it exercised on voting decisions in the United States. To fulfil this objective, the article is divided into two parts. In the first part, it offers a description of the facts reported by *Observer* and *The New York Times* and analyses the conditions that made this possible in relation to the characteristics of the scientific-technological, business and legal context in which it happened. It is important to stress that this article focuses on the US side of the case, which was the one that garnered the most attention and where more information has been confirmed so far through other sources. On the other hand, given that the publication of the information is still very recent and that these are not proven facts, it should be stressed that the argumentation presented in this study does not depend on the veracity or accuracy of the deeds but on an analysis of the conditions that made them possible. Through this analysis, I am seeking to explain that far from being the cause of the problem, this case is its expected consequence. The second part focuses on the possible influence of the Cambridge Analytica case. Following the same logic as in the first part, in the second I explain the kind of influence that the technique of micro-targeting exerts on people. Then, the level of this influence on the US vote is questioned in relation to the limitations of the model used to develop the profile of the target audience of that campaign on the one hand, and according to the current media and sociopolitical context within which the case falls on the other.

In order to fulfil this objective, three main sources are used: scholarly, journalistic and corporate. Given the theoretical nature of the study, the scholarly output is the most relevant source and serves as the foundation of the argumentation developed. Secondly, journalistic sources are used to explain the Cambridge Analytica case. After consulting a large corpus of news reports, the two published by the *Observer* and one published by *The New York Times* (the media outlets which had the scoop on the case) on the 17th of March 2018 (the day when the case was revealed) were chosen, as they contain more detailed information on the deeds. These three are joined by a fourth source published by *Observer* one year before the leak (7 May 2017), when the newspaper began to reveal relevant information from the confession of an informant who was still shrouded in anonymity. Finally, two kinds of corporate sources were examined: first, the websites of the companies involved (Cambridge Analytica and SCL Group), where they describe their own business model, and secondly notifications and official reports on the case published on Facebook.

Your digital life, Cambridge Analytica and the Trump election campaign

The last Facebook estimation (Schroepfer, 4 April 2018) confirms that in 2014 the data of approximately 87 million Facebook users were leaked to the company Cambridge Analytica. Of this 87 million, more than 70 were profiles of US citizens. More than one million of the remainder were citizens of the United Kingdom, and almost 137,000 were Spaniards.

Data collection

According to the testimony of a former Cambridge Analytica and SCL Group employee, Christopher Wiley, published by *Observer - The Guardian* (Cadwalladr & Graham-Harrison, 17 March 2018; Cadwalladr, 17 March 2018) and by *The New York Times* (Rosenberg, Confessore & Cadwalladr, 17 March 2018), the transfer of these data would have taken place thanks to the involvement of Cambridge University professor and researcher Aleksandr Kogan. He would have replicated the *myPersonality* application developed by his colleagues in the Psychology department, whose results were disseminated in a scholarly publication in 2012 (Stillwell & Kosinski 2012). The replica seems to have been *This is Your Digital Life*, a personality test available on Facebook since 2014, which required its participants to have a Facebook account and be US voters. When participating, the users consented to allow the data in their account to be used for academic research, and in exchange they received monetary compensation. According to the data that Zuckerberg made public (21 March 2018), almost 300,000 people performed the test. However, *This is Your Digital Life* also gave Kogan access to certain information on the "friends" of the majority of participants in the test, in such a way that the number of user profiles whose data he obtained increased exponentially to 87 million. Because these "friends" had not consented to his accessing their profiles, the data obtained from them were fundamentally those generated by their participation in the social media, which are usually "public by default".

According to Wiley (Cadwalladr & Graham-Harrison, 17 March 2018), Kogan would have leaked these data to Cambridge Analytica in 2015 via a commercial agreement between his company Global Science Research (GSR) and SCL Elections, a

subsidiary of SCL Group, which is, in turn, a company affiliated with Cambridge Analytica. This leak was not discovered by Facebook until approximately one year later, in 2015, and it then failed to inform either its affected users or the States about the leak.

The recent reports and official publications shared by the Facebook authorities (Grewal, 16 March 2018; Schroepfer, 4 April 2018; Zuckerberg, 21 March 2018) confirm Wiley's testimony. Now, the Facebook Help Centre has made available to users the tool called "How to check if your Facebook data was used by Cambridge Analytica" (Facebook 2018), where they can check whether the data company had accessed the information in their profile.

Data analysis

Wiley would have used the method developed by Stillwell and Kosinski (2012), Kosinski, Stillwell and Graepel (2013) and Youyou, Kosinski and Stillwell (2015) to conduct psychometric studies based on the data obtained from *myPersonality* (Stillwell & Kosinski 2012) to analyse the data collected via *This is Your Digital Life*. Kosinski, Stillwell and Graepel (2013) demonstrated the possibility of ascertaining highly sensitive personal attributes and characteristics by automatically analysing easily-accessible digital records of human behaviour, in this case "likes" on Facebook. The attributes the study demonstrated it could predict include sexual, political and religious orientation, sex, ethnicity and information on users' lives such as drug consumption, level of life satisfaction and whether or not a person's parents remained together until the individual was 21 years old. From this, Wiley would have gotten a description of the psychological profiles of millions of users involved, including their political affinities. The results of the personality test performed by the almost 300,000 people who participated in *This is Your Digital Life* would have been the control group to test the validity of the analyses performed on the entire data set.

According to the information published by The Guardian (Cadwalladr, 7 May 2017), Cambridge Analytica would have combined this psychological information extracted from databases of consumers and then crossed it with postal addresses, emails and telephone numbers. Until that time, Facebook itself allowed profile searches based on telephone numbers or addresses, an option which, as Schroepfer explained (4 April 2018), the company has now deactivated due to the abuses perpetrated by ill-intentioned users.

Data exploitation

The former Cambridge Analytica employee revealed that these data would have been used in a political micro-targeting campaign with the goal of influencing voting decisions during the 2016 presidential elections in favour of Donald Trump (Cadwalladr, 17 March 2018).

Newman (2016) claims that the micro-targeting technique was used in the Obama campaign committees in the 2008 and 2012 presidential elections. Micro-targeting is a direct advertising technique which allows more persuasive campaigns to be generated by using big data analytics techniques and artificial intelligence mechanisms to get information and target the audience in a more personalised fashion (Alkış & Taşkaya Temizel 2015; Miralles-Pechuán, Ponce & Martínez-Villaseñor 2017; Neumann 2017).

However, in the Trump campaign, Christopher Wiley (Cadwalladr, 17 March 2018) points to the use of psychological operations (PSYOPS), a kind of military information warfare technique that seeks to exert a manipulative, not persuasive, influence. PSYOPS are a type of attack which consists in locating targets that are particularly vulnerable to psychological impact and launching a message that is capable of changing their feelings in order to urge them towards a particular action that favours national or allied interests. The US defence forces have waged this kind of information attack before, during or after wars and conflicts (United States Air Force 1999). The research undertaken by Briant (2018) argues that after the terrorist attack waged by Al Qaeda on the 11th of September 2001, the US government decided to extend the use of psychological operations to modern propaganda systems inside the country. In her article, Briant argues that this transformation is due largely to the spread of information and communication technologies which challenge the influence of the propaganda model traditionally used by the US Bureau of Public Affairs. Sartonen, Simola, Timonen and Lovén (2017), in turn, underscore that one of the major potentialities of the psychological profiles yielded from the analysis of online behaviour is their ability to contribute to the objectives of *PSYOPS*.

The case, possible and necessary

First of all, in order to keep in mind the facts we are discussing, it should be noted that if Wiley's testimony is confirmed:

1. There would have been a massive data leak of Facebook users by means of a commercial agreement between the Cambridge University scholar Aleksandr Kogan and SCL Group.
2. In total, this leak would have affected the profiles of approximately 87 million Facebook users.
3. As a consequence, Facebook would have failed to fulfil its rule which requires anyone who gathers user data to inform users of the purpose and not to allow the data to be transferred to third parties. In the case of the affected European countries, Facebook would also have failed to comply with the European Data Protection Regulation (EU 2016/679), which bans the sale of data to third parties.
4. Furthermore, the agreement reached with users who participated in *This is Your Digital Life* would have been violated, as they only consented to provide access to their profile information for academic uses.
5. Subsequently, these data would have been used to

manipulate the voting decision of the US electorate in favour of the candidacy of Donald Trump through a micro-targeting campaign based on military information warfare techniques.

Despite the existence of reports that would, at least, partially confirm Wiley's testimony, the argumentation developed in this study does not depend on the veracity or accuracy of the data but on the existence of the scholarly research that that makes these deeds possible, a business model that needs them and a legal context that is incapable of dealing with it.

Thus, this section explains the main characteristics of the scholarly research, the business model and the legal context related to the case.

Data exploitation as an academic research line

Firstly, the scholarly publications mentioned in the previous section, which are essentially associated with the fields of Psychology, Computational Science and Communication, demonstrate:

1. That the automatic analysis of easily-accessible digital records on the behaviours of people in their social networks reveals a range of sensitive characteristics about their personality, including their political affinity (Kosinski, Stillwell & Graepel 2013; Stillwell & Kosinski 2012; Youyou, Kosinski & Stillwell 2015).
2. That based on the psychological profile obtained in the previous analysis, it is possible to develop more persuasive personalised communication strategies (Alkış & Taşkaya Temizel 2015; Miralles-Pechuán, Ponce & Martínez-Villaseñor 2017; Neumann 2017).
3. That people's psychological profile is of great interest in the application of military emotional manipulation techniques which are capable of modifying people's behaviours based on specific objectives (Sartonen, Simola, Timonen & Lovén 2017).

Due to the social risk entailed in this line of research, it seems essential to clearly stipulate which are its aims for social development and which are the fields in which its practical execution is legitimate.

Data exploitation as a business model

On the other hand, the companies involved in this case, Cambridge Analytica and SCL Group, embody an expanding business model which has the backing of multi-million-dollar investments. This consists in developing strategic communication campaigns whose objective is to modify the behaviour of vulnerable population segments from a given target audience in favour of specific objectives.

Cambridge Analytica (2018) is a company headquartered in New York, Washington and London which was founded in 2013 as a subsidiary of SCL Group. The CEO of the company in the United States, whose biggest investor is the US billionaire Robert Mercer, is Steve Bannon, former Senior White House Counsellor to Donald Trump. Under the slogan "Data drives all we do", Cambridge Analytica presents itself as a company that "uses data to change the audience's behaviour". The company is made up of a sales division devoted to advertising and marketing, and a political division devoted to electoral communication campaigns. The services it offers, whether targeted to consumers or voters, are: researching the target audience in order to learn about it in-depth and understand its main characteristics; adding and integrating the data obtained into a centralised platform; predicting audience segments likely to respond favourably to the messages; developing customised multi-channel campaigns to capture key audience segments; and reporting on their future scope through campaign performance data. It promises companies that they can learn about every individual in their target audience in order to help them connect with them "on a personal level". It promises its clients in the political division to identify their target electorate, learn more about them and gain more influence over them in order to spur them to action at a low cost. In other words, its business model consists in data exploitation to modify the target audience's behaviour.

In turn, SCL Group (2018) also belongs to Robert Mercer, and as stated on its website. It is a company devoted to developing strategic communication campaigns for governments and military organisations all over the world based on data analytics. Its main objective is to spark changes in behaviour in defence, intelligence and social-change operations.

With regard to the business model, therefore, it is essential to ensure that all the companies' private interests respect citizens' rights and the democratic organisation of society.

Legal insufficiency

Finally, if Wiley's testimony is confirmed, there would have taken place alleged illegalities related to data collection. This section shows that, beyond punishing these illegalities, the legal framework of personal data protection is insufficient to deal with the situation. The reflections are common to American and European cases, which are grounded upon the same individual 'notice and choice' model (Baruh & Popescu 2015). This requires people to be clearly informed about what happens to their data, since based on this information, they can provide their consent (or not) to give up the data.

Data accessibility

Given that the bulk of the information that Cambridge Analytica supposedly used to generate a strategy to influence the electorate is easily accessible (likes), the fact that it obtained them illegally does not seem overly relevant.

In this regard, it seems essential to point out the fact that just because the data are accessible does not mean that they are public. Social media interfaces are spaces designed and managed by private companies with certain commercial interests, and therefore they are not exactly comparable to

traditional public spaces. Besides, the fact that something is public does not mean that it can be used by anyone or for any purpose.

Invalid agreement

Likewise, by lying about the purpose of the data (commercial, not scholarly), there would have been a rupture in the agreement between the two parties: the research who asks for the user's consent to collect their data, and the user who provides it. Beyond this rupture in the agreement, which was punished by the social media itself, the Cambridge Analytica case shows that, as argued in a previous study (Suárez-Gonzalo 2017), individual consent is an invalid instrument to protect personal data, at least for these reasons:

1. It is a requirement to participate in and enjoy products and services. In the case of *This is Your Digital Life*, users had to accept the user conditions of both the Internet browser and those of Facebook and the application itself. Furthermore, in this case the cession of data seems to have been associated with monetary compensation.
2. Due to the capacity of big data analytics technologies to infer latent information in data, users consent to provide access to certain data in their profile but remain unaware of what sensitive information can be gotten by analysing these data (Tufekci 2015). This means that even though the footprints of our basic behaviour as social media users are not necessarily considered personal data, the information that can be extracted from analysing them can become extremely sensitive.
3. On the other hand, the personal information that a person disseminates also affects others, so a person is not necessarily aware of (or has not necessarily consented to) the publication of information that affects them. In this sense, individual consent has a social impact. The case of *This is Your Digital Life* exemplifies this issue in two ways. First, the fact that a group of people participated in the test has been used to harm millions of other people who have nothing to do with it. Secondly, the fact that these people gave their consent helps to shape a business model based on the exploitation of personal information that affects society as a whole.
4. This complexity is compounded by the intentional opacity of big data technologies (Pasquale 2015), which makes it particularly complex for people to be properly informed about what will happen to their data when they consent. This also means that the agreement reached via consent does not entail negotiation, nor does it take place between equal parties.

For these reasons, it is difficult to consider individual consent a valid method to protect personal data.

The influence, in its context

The section above focused on the characteristics of the context in which the Cambridge Analytica case occurred. This section focuses on the context related to the type and level of influence of the case.

Given the seriousness of the facts revealed, there is no doubt that a rigorous study of the veracity of the deeds and their level of influence on Donald Trump's victory is needed. However, focusing our attention exclusively on this matter may be futile, firstly because it is difficult to measure the level of influence that an isolated act has within a complex decision. Secondly, because this could lead us to minimise the importance of the fact that there is a business precisely model devoted to gaining this influence, and furthermore, because if big data technology continues developing in the same way as today, its capacity for influence will continue to grow.

The purpose of this section is to explain the importance of focusing on the social impact of the system which makes possible the Cambridge Analytica case, instead of the specific interference of the case in US voting decision. To do so, this section describes the kind of influence that micro-targeting technique exerts over people. It then questions this influence, on the one hand, in relation to the limitations of the model used to devise the profile of the target audience of that particular campaign and, on the other, in accordance with the current media and sociopolitical context of the case.

Persuasion or manipulation

According to Bennett (2015), the technique of micro-targeting incorporates the trends that are characteristic of current electoral campaign management in Western societies, such as: it uses big data technologies to collect and integrate the data on voters into unified management platforms, including their consumption data and the data generated on the social media, and it signals the shift from mass messages to targeting micro-audiences. Bennett claims that these techniques emerged as the outcome of the decreasing efficacy of traditional techniques. They are cheaper yet more intrusive ways of influencing voters' behaviours. He also notes that these trends are generating a consumerisation of the vote, and therefore they not only affect the individual's privacy but also broader democratic dynamics.

By defining an individualised audience profile, the technique of micro-targeting exposes the individual to certain information selectively. In this way, it does not explicitly say what to consume or whom to vote for but instead shapes some of the referents based on which people spend money and vote. Likewise, the fact that the individual is unaware which of their profiles the person targeting them is using when exposing them to this information places them in a position of being vulnerable to manipulation.

Yet another issue is the fact that Wiley's testimony cites the use of military techniques with a psychological impact. Even though this has not been proven, there are two factors that lead us to

mistrust it. On the one hand, the notable similarity between the range of services purveyed by the company Cambridge Analytica (2018) and the characteristics of the information attacks perpetrated by the US defence forces (United States Force 1999). On the other hand, the experience of SCL Group (2018) in developing strategic defence campaigns and its association with the military elites. This is joined by scholarly studies that show the potentiality of psychological profiles to undertake "psychological operations".

Biased profile

Micro-targeting is based on defining a precise, individualised profile of the target audience. In the case of the Trump campaign, this profile was devised based on the model developed by Cambridge University (Kosinski, Stillwell & Graepel 2013; Stillwell & Kosinski 2012; Youyou, Kosinski & Stillwell 2015). In this sense, when discussing the influence of the Cambridge Analytica case, it is essential to weigh the possible limitations of this model.

Big data technologies provide an overview of what is being studied, that is, a broad picture of the situation. What is not as clear is that through this picture is it possible to understand or explain complex phenomena such as psychology and human behaviour, which are not mathematical (Boyd & Crawford 2012). For this reason, it seems essential with a touch of scepticism the assumption that through the analysis of a given representation of human behaviour (likes), precise information can be gained on complex personality features (ideology). In this sense, the application of big data analytics to human behaviour as in the case of *This is Your Digital Life* may mean that the profiles developed are biased. In this way, the potential influence exerted by the Trump campaign would be diminished.

Media context

The aim here is to relate the possible influence of the Cambridge Analytica strategy on the US decision to vote for Trump or Clinton with the current media context in which the US election campaign took place.

In a representative democratic system, freedom to elect political representatives is crucial. This requires, among other things, that citizens have access to truthful, diverse and plural information. For this reason, the traditional media, as well as the new social media, should be democratising tools serving the right to freedom of expression. However, media manipulation and disinformation are on the rise, and as a result the credibility of the media is being called into question (Marwick & Lewis 2017; HLEG 2018).

Marwick and Lewis (2017) argue that disinformation online and ideological radicalisation are consequences of online media manipulation. As the result of a deterioration in trust in the traditional media, the main actors in media manipulation (trolls, gamergaters, conspiracy theoreticians, influencers, haters, hyper-partisan news media and politicians) have found their space in blogs and websites, forums and message boards on the Internet and in the leading social media (such as Facebook, YouTube and Twitter). According to the authors, they are generally motivated by reasons related to ideology, money or the quest for status or acceptance. Thus, the circulation of memes and hoaxes, conspiracies against candidates, the use of bots and the distribution of fake news also played a major role in the election campaign for the US presidency (Marwick & Lewis, 2017). One example of this was the disinformation campaign promoted online about the Democratic candidate's purported ill health, which went viral and made the leap to the traditional media.

On the other hand, the developments in big data technology and artificial intelligence have led what is called the "algorithm culture" (Hallinan & Striphas 2016) to also affect information classification and hierarchisation. In recent years, the use of search engines on the Internet and the social media to check information has become very common (Nikolov, Oliveira, Flammini & Menczer 2015). During the peak of the US presidential elections, 62% of citizens got their information through the social media (Shearer & Gottfried 2017). Due to the multiplication of devices from which information is accessible, personalised recommendation systems have been developed as the best way to get news contents to Internet users in line with their interests (Yingyuan, Pengqiang, Hsu, Hongya & Xu 2015). Numerous recent studies (Borgesius, Trilling, Möller, Bodó, de Vreese & Helberger 2016; Dutton, Reisdorf, Dubois & Blank 2017; Holone 2016; Nicolov, Oliveira, Flammini & Menczer 2015) have focused on the impact of algorithm culture on the rise of disinformation and media manipulation. The majority concur that citizens are exposed to biased information which confirms and reinforces the thoughts and attitudes that they and people with views like theirs already have. This is known as the bubble effect or echo chambers.

On the other hand, the traditional media still play an important role in electoral campaigns. According to Marwick and Lewis (2017), the framing and strategic amplification of certain ideas or messages is one of the most common media manipulation techniques. Patterson (2016) states that the tone used in the media coverage was overwhelmingly negative, while the discussion of political issues was extremely light. However, he also concludes that the candidate Hillary Clinton was treated more negatively than her political rival. Foster, Shoaf and Parsons (2016) claim that gender stereotypes continue to harm female candidates in the media coverage of electoral campaigns. Likewise, the construction of the political frameworks (Oates & Moe 2016) or the different ways the candidates used the social media (Enli 2017) also played a major role in the electoral campaign.

This media context reveals at least three interesting issues which can help us assess the possible influence of the Cambridge Analytica case. First, it shows that the micro-targeting campaign waged by Cambridge Analytica is framed within the new forms of media manipulation related to the bubble effect. Secondly, this would not be the only influence

strategy to which citizens were exposed during the campaign. And finally, the interests of Trump and Cambridge Analytica were not isolated from the interests of the other actors and media influencing the campaign.

Social and political context

The explanations suggested for Trump's victory include many others that are not solely related to the media's actions. According to Gaughan (2016), some of them are related to the economic concerns of white working-class voters (which the Trump campaign managed to identify); the rise of racism and misogyny; the segregation and polarisation of the electorate (which, as seen in the previous section, could be related to media manipulation); the increase in income inequality; and the controversial actions of the FBI director. Thus, another important issue when discussing the influence of the Cambridge Analytica case is the political and social context in which the electoral campaign occurred. Fraser (2017) claims that Trump's win is part of a series of political events that have recently occurred worldwide. They include the triumph of Brexit, Bernie Sanders' campaign in the Democratic Party primaries in the US, the rejection of Matteo Renzi's reforms in Italy and the increased support of Marine Le Pen's National Front in France. These events, explains Fraser, represent citizen pushback to the effects of globalisation, as well as to a new form of "progressive neoliberalism" and the ruling classes that have promoted it. Trump, Fraser says, captured part of the electorate thanks to a "reactionary populism" which was opposed to the mixture of truncated ideals of emancipation and lethal forms of financialisation represented by "progressive neoliberalism".

Conclusions

The argumentation throughout this article gives rise to at least the following conclusions:

1. The Cambridge Analytica case is the probable consequence of a given scientific-technological structure, a business model and a legal framework that make it possible and necessary.
2. Focusing attention on the level of influence that the Cambridge Analytica strategy may have had in the US voting decision is not useful in helping us understand the seriousness of the situation for these four reasons: it deflects attention from the structures sustaining the case and its social impact; the influence of a specific act on a complex decision is difficult to measure; the very biases of the method used to develop this strategy could reduce this influence; and it would be relative to its media, social and political context.
3. The possible influence exerted by the micro-targeting technique used by Cambridge Analytica falls within a broader phenomenon of media manipulation bounded to new technologies and the bubble effect that has been proven to be an important reason behind the rise of online disinformation and the radicalisation of political ideas and opinions.

The Cambridge Analytica case reveals that the current development of big data technologies is generating a power inequality between citizens and a group that exercises despotic power over information and data exploitation. This affects fundamental rights like privacy, personal data protection and the right to information, as well as the democratic quality of states. For this reason, this study points out the need to:

1. Reconsider the social fitting of the structures that catalyse events like the one waged by Cambridge Analytica.
2. To not lose sight of the social and political impact of big data technologies.
3. Rethink the legal framework of personal data protection to correct its insufficiencies.
4. Establish mechanisms that allow society as a whole to have information and control mechanisms over big data technologies.
5. Impose limits, if needed, to forms of big data exploitation and/or uses that are harmful for society as a whole.

References

Alkış, N.; Taşkaya Temizel, T. "The impact of individual differences on influence strategies. *Personality and Individual Differences, 87*(2015), 147-152. doi: 10.1016/j.paid.2015.07.037.

Baruh, L.; Popescu, M. "Big data analytics and the limits of privacy self-management". *New Media & Society*, Vol. 19, no. 4, (2015), 579-596. doi: 10.1177/1461444815614001.

Bennett, C. J. "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications". *Surveillance & Society, 13*(3/4), (2015), 370-384.<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv>

boyd, d.; Crawford, K. "Critical questions for big data", *Information, Communication & Society, 15*(5), (2012), 662-679. doi: 10.1080/1369118X.2012.678878.

Borgesius, F. J.; Trilling, D.; Möller, J.; Bodó, B.; de Vreese, C. H.; Helberger, N. "Should we worry about filter bubbles?" *Internet Policy Review, 5*(1), (2016). doi: 10.14763/2016.1.401.

Briant, E. L. "Pentagon Ju-Jitsu – reshaping the field of propaganda". *Critical Sociology (5 March 2018)*, 1-18. doi: 10.1177/0896920517750741.

Cadwalladr, C. "'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower". *Observer – The Guardian,* 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump> [Retrieved: 23 April 2018].

Cadwalladr, C. "The great British Brexit robbery: How our democracy was hijacked". *Observer – The Guardian*, 7 May 2017. <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> [Retrieved: 23 April 2018].

Cadwalladr, C.; Graham-Harrison, E. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *Observer – The Guardian*, 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [Retrieved: 23 April 2018].

Cambridge Analytica. *Cambridge Analytica*. 2018. <https://cambridgeanalytica.org/> [Retrieved: 23 April 2018].

Dutton, W. H.; Reisdorf, B. C.; Dubois, E.; Blank, G. "Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News". *Quello Center Working Paper No. 2944191*. (2017), 1-26. doi: 10.2139/ssrn.2944191.

Enli, G. "Twitter as arena for the authentic outsider: exploring the social media campaigns of Trump and Clinton in the 2016 US presidential election". *European Journal of Communication*, *32*(1), (2017), 50-61. doi: 10.1177/0267323116682802.

Facebook. "¿Cómo puedo averiguar si se ha compartido mi información con Cambridge Analytica?". *Servicio de ayuda de Facebook*, 2018. <https://www.facebook.com/help/1873665312923476> [Retrieved: 18 April 2018].

Foster Shoaf, N.; Parsons, T. N. "18 Million Cracks, but No Cigar: News Media and the Campaigns of Clinton, Palin, and Bachmann". *Social Sciences, MDPI, Open Access Journal,* 5(3), (2016), 1-15. <https://ideas.repec.org/a/gam/jscscx/v5y2016i3p50-d78592.html>

Fraser, N. "Progressive Neoliberalism versus Reactionary Populism: A Choice that Feminists Should Refuse". *NORA - Nordic Journal of Feminist and Gender Research, 24*(4), (2017), 281-284. doi: 10.1080/08038740.2016.1278263.

Gaughan, A. (2016). "Explaining Donald Trump's Shock Election Win". *Scientific American*, 9 November 2016. <https://www.scientificamerican.com/article/explaining-donald-trump-s-shock-election-win/>

Grewal, P. "Suspending Cambridge Analytica and SCL Group from Facebook". *Facebook Newsroom*, 16 March 2018. <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/> [Retrieved: 18 April 2018].

Hallinan, B.; Striphas, T. "Recommended for you: The Netflix Prize and the production of algorithmic culture". *New Media & Society*, 18(1), (2016), 117–137. doi: 10.1177/1461444814538646.

Hargittai, E.; Marwick, A. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy". *International Journal of Communication*, *10*(2016), 3737–3757.

High Level Group on Fake News and Online Disinformation. *A multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation*. 2018. <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. [Retrieved: 13 March 2018].

Holone, H. "The filter bubble and its effect on online personal health information". *Croatian Medical Journal, 57*(3), (2016), 298–301.

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

Marwick, A.; Lewis, R. *Media Manipulation and Disinformation Online*. *Data & Society Research Institute*, 2017. <https://datasociety.net/output/media-manipulation-and-disinfo-online/>.

Miralles-Pechuán, L.; Ponce, H.; Martínez-Villaseñor, L. "A novel methodology for optimizing display advertising campaigns using genetic algorithms". *Electronic Commerce Research and Applications*, *27*, January-February 2018, 39–51. Published online for the first time in November 2017. doi: 10.1016/j.elerap.2017.11.004.

Neumann, N. "The power of big data and algorithms for advertising and customer communication". *International Workshop on Big Data and Information Security, IWBIS 2016, art. nº 7872882*, 2017, 13-14. doi: 10.1109/IWBIS.2016.7872882.

Newman, B. I. *The Marketing Revolution in Politics: What Recent U.S. Presidential Campaigns Can Teach us about Effective Marketing*. Toronto: University of Toronto Press, 2016, 224 pages.

Nikolov, D.; Oliveira, D. F. M.; Flammini, A.; Menczer, F. "Measuring online social bubbles". *PeerJ Computer Science*, *1*(e38), (2015). doi: 10.7717/peerj-cs.38.

Oates, S.; Moe, W. W. "Donald Trump and the 'Oxygen of Publicity': Branding, Social Media, and Mass Media in the 2016 Presidential Primary Elections". *American Political Science Association Annual Meeting 2016*. doi: 10.2139/ssrn.2830195.

European Parliament. *Resolution of the European Parliament dated 14 March 2017 on fundamental rights implications of big data: privacy data protection, non-discrimination, security and law-enforcement* (2016/2225(INI)). <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES>

European Parliament; Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and Council, dated 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation").* <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>.

Pasquale, F. *The Black Box Society. The Secret Algorithms that Control Money and Information*. London: Harvard University Press, 2015.

Patterson, T. "News Coverage of the 2016 General Election: How the Press Failed the Voters". *Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School*, 7 December 2016. <https://shorensteincenter.org/news-coverage-2016-general-election/>.

Rosenberg, M.; Confessore, N.; Cadwalladr, C. "How Trump Consultants Exploited the Facebook Data of Millions". *The New York Times*, 17 March 2018. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [Retrieved: 23 April 2018].

Sartonen, M.; Simola, P.; Timonen, J.; Lovén, L. "Cyber personalities as a target audience". *European Conference on Information Warfare and Security, ECCWS,* 2017, 411-418. <https://www.semanticscholar.org/paper/Cyber-Personalities-as-a-Target-Audience-Sartonen-Simola/1cc84c9b9ad74e426aee32828e17c54adad7246a>

Schroepfer, M. "An Update on Our Plans to Restrict Data Access on Facebook". *Facebook Newsroom*, 4 April 2018. <https://newsroom.fb.com/news/2018/04/restricting-data-access/> [Retrieved: 18 April 2018].

SCL Group. *SCL Group*. <https://sclgroup.cc/home> [Retrieved: 23 April 2018].

Shearer, E.; Gottfried, J. "News Use Across Social Media Platforms 2017". *Pew Research Centre*, 2017. <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/> [Retrieved: 23 April 2018].

Stillwell, D.J.; Kosinski, M. "myPersonality project: Example of successful utilization of online social networks for large-scale social research", *International Conference on Mobile Systems (MobiSys) 2012.* <www.michalkosinski.com/Stillwell_and_Kosinski_2012.pdf>.

Suárez-Gonzalo, S. "Big social data: límites del modelo *notice and choice* para la protección de la privacidad", *El profesional de la Información, (26)*2, (2017), 283-292. doi: 10.3145/epi.2017.mar.15.

Tufekci, Z. "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency". *Colorado Technology Law Journal (13)*, (2015), 203-218.

Turow, J.; Hennessy, M.; Draper, N. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up to Exploitation".* Annenberg School for Communication University of Pennsylvania, 2015. <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>.

United States Air Force. *Psychological Operations. Air Force Doctrine Document 2-5.3. 27 August 1999*. <http://www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf> [Retrieved: 19 April 2018].

Yingyuan, X.; Pengqiang, A. I.; Hsu, C.; Hongya, W.; Xu, J. "Time-Ordered Collaborative Filtering for News Recommendation". *China Communications, 12*(12), (2015), 53-62. doi: 10.1109/CC.2015.7385528.

Youyou, W.; Kosinski, M.; Stillwell, D. J. "Computer-based personality judgments are more accurate than those made by humans". *Proceedings of the National Academy of Sciences of the United States of America*, 112(4), (2015), 1036-1040. doi: https://doi.org/10.1073/pnas.1418680112.

Zuckerberg, M. "I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue". *Publication on Facebook*, 21 March 2018. <https://www.facebook.com/zuck/posts/10104712037900071> [Retrieved: 18 April 2018].