Political micro-targeting: a European information war story

The principle of transparency and algorithmic decision-making in politics

LL.M Law and Technology 2017-18

Tilburg Law School

Tilburg Institute for Law, Technology, and Society

Tilburg University

Student:

Rita Miguel Vilas Curto

Supervisor:

mr. dr. Colette Cuijpers

Acknowledgments:

I would like to begin by thanking to my supervisor mr. dr. Colette Cuijpers, for having guided me through the challenge that was writing this thesis with comprehension, patience and kindness. I would also like to thank to mr. Shazade Jameson for her challenging thoughts and critics, which have truly helped me to explore and develop my line of though.

To my whole family and to my parents, Florbela, João and Vitor, that always encouraged me to follow my dreams and made me believe I could accomplish anything. To my lifetime friends but, especially to my new friends that were my second family in the Netherlands. To José Esfola, my "big brother" and to Tomás Paulo, with whom I had the most enlightening discussions about my topic, my doubts and even my life.

This work is dedicated to all of you.

Table of Contents

1. Introduction

1.1. Background

The predictability of human behaviour has been scientifically established as an existing phenomenon.[1] Nevertheless, behavioural predictability, has been further fuelled by monumental advances in technology and the precise analysis of massive amounts of data harboured by such technologies and hence, leveraged by social media. After logging in, Facebook asks you "What's on your mind?", subscribing to this premise leaves an immutable "digital footprint",[2] thus opening doors of tracking and observation of human behaviour, due to the wide production of data by the usage of virtual networking and the consequent processing of that data. Such occurrence has recently been eloquently discussed regarding the profiling of individuals by political parties in the United States[3] and the UK,[4] a practice which became part of the European socio-political trends.[5]

Barack Obama's campaign is a classic tale of the Internet's significance in political campaigning that led to a profound dependence on social media and consequently data analytics, both in 2008 and 2012.[6][7] The constitutional framework of the U.S. favours the free access to personal data for political campaigns,[8] and thus constitutional leverage played a great role, more recently, in Donald Trump's political campaign,[9] where its promoters used Facebook to project

[1] C. Song and others, 'Limits of Predictability in Human Mobility' (2010) 327 Science.
[2] *The End Of Privacy, Keynote At Cebit'17* (2017). https://www.youtube.com/watch?v=DYhAM34Hhzc&feature=youtu.be.
[3] April Glaser, 'Potential Lawsuit Could Reveal How Trump Targeted Voters On Facebook And If There'S Any Connection To Russia' <http://www.slate.com/blogs/future_tense/2017/10/06/possible_british_lawsuit_could_reveal_how_cambridge_analytica_targeted_voters.html> accessed 18 November 2017.
[4] Jamie Doward and Alice Gibbs, 'Did Cambridge Analytica Influence The Brexit Vote And The US Election?' *The Guardian* (2017).
[5] Colin J. Bennett, 'Voter Databases, Micro-Targeting, And Data Protection Law: Can Political Parties Campaign In Europe As They Do In North America?' (2016) 6 International Data Privacy Law.
[6] Colin Bennett, 'The Politics Of Privacy And The Privacy Of Politics: Parties, Elections And Voter Surveillance In Western Democracies' [2013] SSRN Electronic Journal.
[7] Michael Scherer, 'Friended: How The Obama Campaign Connected With Young Voters' [2012] *Time*.
[8] Colin J. Bennett, 2016: 263.
[9] Colin J. Bennett, 2016: 262.

targeted ads to voters based on the availability of personal data by users.[10] Nonetheless, the fascination of targeted virtual political campaigning was not limited to the U.S. but observed in European context. The UK also could not resist succumbing to this trend, where social network influence and the associated new campaigning techniques were hotly debated concerning 2016's Brexit campaign. Accordingly, if once it was only a strong suspicion that the information provided on such platforms triggered the processing of personal data by political parties in European countries,[11] today it is a certainty that social media is used to build "psychological warfare tools" that impact political campaigns.[12]

To substantiate the affirmation presented above, there were not only availability of general patterns but also preliminary assessment via existing literature available about the nature and extent of voter *dataveillance*[13] - meaning data surveillance, a type of surveillance at issue when the data revealed by the subjects is "collected, aggregated and stored in databases by a variety of data controllers, who can integrate them with other databases, mine them at any time and sell them to other interested parties",[14] which constitutes a preliminary process to engage in contemporary political campaigning practices by political parties, following the above described trends. Such information emerged mostly in the U.S., but it arose also in a smaller scale, in Europe[15] even though data surveillance is normally kept in secrecy. However, in March 2018 the whistle-blower, Christopher Wylie, exposed 'Cambridge Analytica', the company behind not only Trump's campaign but also Brexit's, revealing how personal data on the electorate was collected from Facebook, and further used to create individual profiles on voters to target them with personalised political advertisement, a purpose different from the one for which the electorate authorised the access to their data in first place.[16] The main goal of the software that allowed personalisation of

[10] Carole Cadwalladr, ''I Made Steve Bannon'S Psychological Warfare Tool': Meet The Data War Whistleblower' *The Guardian* (2018).
[11] Jamie Doward and Alice Gibbs, 2017.
[12] Carole Cadwalladr, 2018.
[13] Mireille Hildebrandt, 'Profiling And The Identity Of The European Citizen', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010) (1).
[14] *ibid.*
[15] Tom Dobber and others, 'Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques' (2017) 6 Internet Policy Review <http://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-politicalbehavioural-targeting> accessed 7 January 2018.
[16] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 5 April 2018 (1).

propaganda was to 'predict and influence choices at the ballot box',[17] to 'identify possible swing voters and craft messages more likely to resonate', in line with the results obtained in a psychology study.[18]

As stated in the opening line, human behaviour is largely predictable and as mentioned in the study above quoted, the researchers managed to show that through synthesis and analysis of personal data, the personality behaviour and interests of individuals are predictable with a high level of accuracy, including their political opinions. Subsequently, drawing on huge amounts of data deemed insignificant at first sight, consistent correlations between 'likes' and individual's characteristics were found, and laid the foundation for creating an algorithm that 'could analyse individual Facebook profiles and determine personality traits linked to voting behaviour'[19][20] to construct tailored profiles for endorsement of individuals' interests and beliefs.[21] Through these revelations, 'political micro-targeting', the ultimate political weapon that was for a long time kept in secret was disclosed, and the powerfulness of the merger between algorithms and a large database is witnessed everyday around the world.

Notwithstanding this, other than the American Presidential elections, during which the use of data for political campaigning is well known and the Brexit's referendum, now under the media "spotlight", the influence of such political technique throughout Europe has been questioned.[22] Nonetheless, recent studies on the Dutch and German elections have provided useful information that allow us to affirm the unbridled use of technology and its achievements in elections in Europe.[23][24] Therefore, given the strong evidence of the technological development in politics,

[17] Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[18] Carole Cadwalladr and Emma Graham-Harrison, 'How Cambridge Analytica Turned Facebook 'Likes' Into A Lucrative Political Tool' *The Guardian* (2018) <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> accessed 5 April 2018 (2).
[19] Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[20] About the data gathered by the algorithm used to profile the electorate in the 'Cambridge Analytica' case: 'It trawls through the most apparently trivial, throwaway postings (…) to gather sensitive personal information about sexual orientation, race, gender, even intelligence and childhood trauma'. In Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[21] *ibid.*
[22] Colin J. Bennett, 2016.
[23] Tom Dobber and others, 'Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques' (2017) 6 Internet Policy Review <http://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-politicalbehavioural-targeting> accessed 7 January 2018.
[24] Simon Kruschinski and Andre Haller, 'Restrictions On Data-Driven Political Micro-Targeting In Germany' (2018) 6 Internet Policy Review <https://policyreview.info/articles/analysis/restrictions-data-driven-political-micro-targeting-germany > accessed 7 January 2018.

translated into political micro-targeting practices entrenched in political campaigning in Europe, it is crucial to proceed with a discussion on the legal constraints according to the European legislative framework, particularly on data protection law since these practices are dependent on personal data of the electorate.

1.2. Defining the problem of political micro-targeting

The elections are a vibrant public debate, it is during the political campaign that the candidates are able to demonstrate their 'flags' in order to reach the public and ultimately win the election. However, to win an election first the candidate has to "win the public". To this end, data on the preferences of the electorate have always been crucial. In the past the processing of data relied only on mechanisms such as, voter registry or demographic censuses to provide information on mass audiences however, currently, with the development of communication technologies and the dissemination of internet and social media, data analytics became the most powerful weapon of the political parties,[25] allowing for a deeper and better understanding of the electorate.

Over time due to the technological advancement, the political campaign techniques shifted from stand-alone voter management databases to more integrated voter management platforms (called "the campaign in a box"); the increasing and more unstructured capture of user-generated data from social media; the development of mobile applications for political messaging and campaigning and hence from mass messaging to micro-targeting, including the integration of personal data from commercial data brokerage firms.[26]

In view of the above, the campaigning technique of political micro-targeting emerged, being defined as a "relatively new form of political direct marketing in which political actors target personalized messages to individual voters by applying predictive modelling techniques to massive troves of voter data".[27] This mollycoddling by politicians can therefore not only lead to

[25] "Documents seen by the *Observer*, and confirmed by a Facebook statement, show that by late 2015 the company had found out that information had been harvested on an unprecedented scale." In Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[26] Colin J. Bennett, 'Voter Surveillance, Micro-Targeting And Democratic Politics: Knowing How People Vote Before They Do' [2014] SSRN Electronic Journal.
[27] Ira Rubinstein, 'Voter Privacy In The Age Of Big Data' [2014] SSRN Electronic Journal.

'broadcasting' their messages to the public but also enable them to precisely understand the needs of voters, and to predict voting habits, allocating their resources more efficiently to 'narrowcast' messages tailored to the voter's intimate preferences.[28]

The perils of using predictive modelling techniques, based on personal data in political campaigns to secretly target the electorate might be highly invasive according to data protection law, the framework that sets the limits on data processing, having a huge impact on citizens' rights as voters, since political micro-targeting is highly dependent on the electorate's personal data. Most of the times, the data used in new campaigning techniques is emitted directly by the individuals without them even being aware of the possibility to build a profile on their information or determining, for instance, political opinions through aspects such as, demographic, geographic, psychographic and behavioural.[29] Even less are the voter's aware of how those profiles might be used to target them individually, with political messages envisaged to appeal to their personal characteristics, bearing not only a risk to the individual's right to data protection[30] but also, ultimately, a risk to the democratic system, the risk of voter manipulation. [31]

The 'Cambridge Analytica' case demonstrated that "The predictability of individual attributes from digital records of behaviour… (…) can easily be applied to large numbers of people without their individual consent and without them noticing…"[32] The opaqueness evident in such processes, embedded in complex algorithms, leaves the individual unaware of being surveilled and even less profiled and targeted. It is an invasion of one's state of mind when an individual signs up to a virtual networking platform, where the platform uses personal information for purposes that an individual has not signed up for and is not further informed of, thus contributing to the advent of political profiling.[33] Moreover, the regular presence of technical algorithms in the

[28] Colin J. Bennett, 'How Campaign 'Micro-Targeting' Works ? And Why It Probably Doesn't.' *iPolitics* (2015) <http://ipolitics.ca/2015/09/09/how-campaign-micro-targeting-works-and-why-it-probably-doesnt> accessed 18 May 2018.

[29] Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 'Political Marketing In The Times Of Big Data' [2017].

[30] Frederik Borgesius and others, 'Online Political Microtargeting: Promises And Threats For Democracy' (2018) 14 Utrecht Law Review: 87.

[31] "Apart from privacy threats, there is a threat of manipulation. Politicians could use microtargeting to manipulate voters. For instance, a party could target particular voters with tailored information that maximises, or minimises, voter engagement." Frederik Borgesius and others, 2018: 87.

[32] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).

[33] 'Social Media: Censorship Against Freedom Of Speech' <https://medium.com/@khalilkafa/social-media-censorship-against-freedom-of-speech-76603634c2d9>.

decision-making embed in political 'micro-targeting' makes the desired transparency harder to guarantee. The algorithms supporting 'micro-targeting' are deemed as effective and precise tools to profile the electorate however, their secrecy and, most importantly, their complexity makes them hardly comprehensible by the public, 'blurring' the possibility of a clear understanding of the decision-making based on algorithms. Moreover, the lack of understanding might increase a transparency deficiency in the process of political 'micro-targeting' and, subsequently, the risks above mentioned.

Pasquale affirmed "Gaps in knowledge, putative and real, have powerful implications, as do the uses that are made of them."[34] The great influence of the social networks in recent elections is noticeable and its effects are remarkable however, the political system, as a crucial element to democracy, must be characterized by openness and transparency, the promotion of public discussion within the community. Differently, political parties are keeping their campaign tactics in secrecy, 'hiding' not only their campaigning processes from the public scrutiny but also the utilisation of the electorate's data in such processes from the strict regulations adjacent to the processing of personal data namely, the transparency obligations in the processing of personal data. Therefore, in a world where the exposure is unavoidable and our data reveal so much, on the hypothesis of 'micro-targeting' being a growing tendency in European electoral politics, the impact of European data protection law in this phenomenon needs to be assessed.[35] It is imperative to know, as voters, how we can uphold our rights when "they hide their actions", creating gaps in the knowledge of the public but, "our own lives are increasingly open books".[36]

1.3. Research questions

Bearing in mind the procedure of political micro-targeting, the purpose of my research is to analyse the transparency constraints imposed on data processing for political campaigning by the General Data Protection Regulation (hereinafter, GDPR) and assess its adequacy to political micro-targeting, a powerful campaigning technique to unravel the electorate most intimate

[34] Frank A Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information* (Harvard University Press 2015), p.2.
[35] Colin J. Bennett , 2016: 261-275.
[36] Frank A Pasquale, 2015: 2.

information that must be clear to the public. So, the central question guiding my thesis is the following: Given that political micro targeting might be a campaigning technique anchored in the most paradigmatic elections in Europe, successful due to the secret processing of personal data on the electorate through complex and accurate algorithms, can the existing European Data Protection Legislation, which establishes obligations of transparency in data processing, ensure a proper balance between the interests of political parties in processing personal data and the electorate fundamental right to the protection of personal data? The answer to this question will eventually find whether, from a data protection perspective, the EU framework, effectively safeguards the voters personal data and their correspondent rights within a democratic system.

To answer the main question however, the following sub-questions must be answered first:

1) Bearing in mind the role of data in contemporary campaigning techniques, is political micro-targeting a current procedure in European politics?
2) Considering the application of the GDPR to political micro-targeting, how is the campaigning technique relevant according to its provisions, with emphasis on the transparency principle?
3) Hence, are there adequate and effective remedies defined in the GDPR towards guaranteeing the voters rights regarding the transparency obligations?
4) What is the best solution according to the GDPR to guarantee the transparency of processing and consequently reassure the electorate's fundamental right to data protection?

1.4. Methodology

About the typology of this thesis, I chose to do a doctrinal/theoretical research. The research is mainly focused in several academic articles that look specifically into the object of research namely, political micro-targeting, a process predominantly characterised by its uncertainty until the revelations of Cristopher Wiley to the Guardian in March 2018.

This research was primarily conducted by the analysis of articles and books of North American scholars, since the phenomenon here portrayed is more common in the U.S. and Canada than in Europe. Therefore, authors like Colin Bennet, Daniel Kreiss, Frank Pasquale and Ira Rubenstein,

determined the starting point into a deep understanding of the logic behind political micro-targeting from a political and legal perspective. To guarantee a high level of certainty to the author's statements in the European political context, the 'Cambridge Analytica' Files by the Guardian are essential documentation to sustain the discoveries and reach conclusions on this dissertation. Once acquainted with the campaigning technique I intend to elaborate on the recent cases studies occurring throughout paradigmatic political campaigns in Europe. So, **chapter 2** starts with an in-depth look at the data practices of contemporary political campaigns, particularly at political micro-targeting. The purpose is to define the concept and exact procedure surrounding the technique, through a detailed focus on how political marketing is nurtured in the digital age and how it is not only a trend in the U.S. but, data analytics as an unsettling reality in politics is also a demarked tendency in Europe. In favour of this hypothesis, the risks implied in political micro-targeting are discussed to emphasize the social and legal problems surrounding such process especially, its transparency deficiency. To this end, an effort is made to define not only the access to this data but also the kind of data accessed by political parties, according to the revealing European case studies.

Established the state of play in the European context, in **chapter 3**, the importance of the European Data Protection framework is highlighted and a descriptive study on the pertinent provisions of the GDPR concerning the dichotomy between the opacity of the campaign system and the transparency obligations enshrined in the GDPR, is carried out and critically applied to the technique and the revealing 'Cambridge Analytica' case, duly included in the investigation as a practical example. In this regard, it is important to note that although at the moment of writing, the Data Protection Directive is still in existence, by the deadline of this thesis, the GDPR will be already in force throughout the EU. Therefore, the application of the new data protection framework is anticipated, even though the old framework and the existing literature in relation to it is still used for interpretation purposes, since the key concepts on the DPD are the same as the one's described under the GDPR.

After the transparency obligations are exposed, considering the adverse impacts of 'micro-targeting', an adequacy and effectiveness assessment is done of the outlined remedies to ensure transparency of the political micro-targeting processes according to the GDPR in **chapter 4**, based on European guidelines and academic articles on the matter.

Finally, newly established solutions to safeguard the transparency of decisions in the GDPR are explored through **chapter 5**, to moderate the impact of political micro-targeting on the democratic system and guarantee the electorate right to data protection. The conclusion of this thesis is anchored in literature and relevant academic papers on the matter, following the case studies revealed in chapter 2.

2. Political Campaigns in the Digital Era

2.1. The importance of political campaigns

Elections give us the opportunity to freely and actively choose our leaders, who will serve the interests of the majority. "They are the core of democracy",[37] whether the election decides the seats in a States Parliament or in a City Council. Irrespectively of the seats at stake, an election has a direct effect on the population. The electorate's choice and ultimate decision over a political party will contribute to its self-development and expression but most of all it will give general acceptance for someone to govern. This creates the need to not only inform but also to promote the public discussion between the candidate's ideas and solutions, giving the best that pluralism has to give, a choice, whether it is the best or not. Therefore, if the elections are the essence of democracy, political campaigning is a vital element of the democratic system. The campaign allows citizens to freely scrutinize the ideas and actions of a candidate or a party and to participate in the selection process, making the "buzz" over billboards, speeches and rallies, television ads and debates or internet pages worthwhile. The openness of the parties towards the public and the transparency of the information provided to the public are crucial in the political system, only a diverse and informed debate pertains to the democratic values.

Through the years, the importance of fair and transparent political campaigns only intensifies. In a world that never stops spinning, the merger of technology and politics has transformed political campaigns.[38] Therefore, this chapter will briefly describe the evolution of practices in political campaigns, highlighting the most remarkable historical events. Then, to show how political campaigning is developed in the digital age, the most relevant campaign practice to the dissertation – political micro-targeting - will be explained in detail. Finally, after establishing the current state of play, the mentioned technique will be defined establishing its connection with today's reality and advancement in political campaigning throughout Europe.

[37] Judith S Trent, Robert V Friedenberg and Robert E Denton, *Political Campaign Communication* (Rowman & Littlefield 2011).

[38] Pippa Norris, 'The Evolution Of Election Campaigns: Eroding Political Engagement?' [2004] Paper for the conference on Political Communications in the 21st Century: 2.

2.2. The influence of technology in the evolution of political campaigning

It is said that "the history of political marketing is actually the political history of the United States from the 1950's".[39] Some moments in history clearly marked a turning point in the way political campaigning is exercised. Those moments can be linked with "the modernization process rooted in technological and political developments common in many post-industrial societies",[40] creating a theoretical framework that divides political campaigning in three significant periods, namely: *pre-modern, modern* and *post-modern*.

Pre-modern campaigns or the *pre-television stage*,[41] started in the 19th century and prevailed until the 1950's as the dominant type of campaigning. This age was mostly characterized for a more direct and personal campaign, at a local level, with short-term, ad-hoc planning by the party leadership. The parties selected the candidates and the contact with the citizens was established by ringing the doorbells, posting pamphlets and targeting the wards. The main source of information was the partisan press although the radio and movies played an important role as well. The electorate was strongly motivated by party identification, proven through the loyalty to the party. Therefore, a local-active campaign[42] was crucial to maintain support.

From the early 1950's to its peak in the mid-1980, **modern campaigns**, were predominantly influenced by television and the publication of regular opinion polling. The communication of political ideas started to be broadcasted in major television channels, turning a local-active campaign into a nationalized one. This feature put the parties in the spotlight, but especially the party leader, the "face of the party", which shifted politics towards its personalization, demonstrating the influence of image over the message and the political program.[43] Therefore, parties started to rely in advertising, marketing, and polling specialists, true advisers external to the party. Consequently, costs increased, creating a gap between the parties with more and less resources. The electorate that was once loyal to a party became devoted to the

[39] Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 2017: 33.
[40] Pippa Norris, 2004: 2.
[41] Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 2017: 35.
[42] A local-active campaign constitutes a campaign conducted through more demanding political activities like rallies, doorstep canvassing, and party meetings.
[43] Pippa Norris, 2004: 3-4.

most charismatic candidate.[44] In contrast with pre-modern campaigns, the participation of citizens became less active, since the biggest concern was the most brilliant way in handling the press, not the citizens.

Reaching the said most recent stage, **post-modern campaigns** are characterized by the maturing of the Internet and subsequently, the new forms that emerge for political parties to communicate with the electorate. The predominant actors marking this revolution in political campaigning are Howard Dean with his online grassroots mobilization, George Bush's online field organization during his re-election bid, but, most importantly,[4546] Barack Obama's two campaigns,[47] where voter modelling and targeting strategies were primarily developed.[48] Nowadays, countless sources inundate citizens with the most varied, complex and incoherent information. The communication between parties and the electorate is permanent and everlastingly scrutinized. Influenced by the fragmentation of sources and by an increased cultural pluralism and social diversity, political marketing assumes great importance. Consequently, campaign advisers and strategists, even on an external level play a role as relevant as the political party itself. Nevertheless, the Internet mechanism flows both ways, allowing voters to determine the course of a campaign while it allows politicians to provide voters with more information tailored to their interests and needs,[49] as demonstrated by recent findings.[50] Political marketing now focuses on the voter's interests as revealed through polls and other techniques. Consequently, strategies are developed to answer the key policy issues identified to maximize the voter's receptiveness. Therefore, one can say campaigning returns to be more local-active and interactive than ever before, even though through different mechanisms.

[44] This period was marked by two key events namely, the beginning of televised debates with the Nixon-Kennedy debate and the election of Ronald Reagan as U.S. President. The latter event emphasized a change of paradigm in political campaigning, moving the focus of the public from the political party to the politician.
[45] Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 2017: 37.
[46] Daniel Kreiss, 'Digital Campaigning', *Handbook of Digital Politics* (Edward Elgar 2018): 118-135.
[47] Colin J. Bennett, 2016: 262-274.
[48] Daniel Kreiss, 'Yes We Can (Profile You): A Brief Primer On Campaigns And Political Data' [2012] *Stanford Law Review Online* <https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/>.
[49] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).
[50] Carole Cadwalladr, 2018.

The forms of communicating with the electorate have changed and so did the mechanisms used to interact with the public that is why it is imperative to unravel the reasons that enabled such change in the next paragraph.

2.3. The ground-breaking role of data in political campaigns

Nowadays, technology is visibly more present in campaigning than before, enabling data-driven campaigns to occur in a much wider scale with an excellence level of accuracy.

Some call it the *fourth stage*[51] in political campaigning, Kreiss[52] called it the *new technology-intensive era* that "reoriented parties and campaigns to the backstage infrastructural technology, data and analytics work"[53] and Nielsen[54] referred to it as a "*personalized political communication*". Nonetheless, all of them commonly agree that a new stage of political campaigning has emerged. The political party's access to data, and the way it is managed, are changing the communication between the parties and the electorate. The tactic nowadays is to invest in individual-based targeting through the analysis of the voter's data, so the allocation of resources by political parties is facilitated and more efficient.[55]

This change in campaigning strategy is associated with events such as the Brexit campaign in the UK[5657] and the 2016 presidential campaign in the U.S.[5859] The substantial change represented in both events took place due to use of the widely available[60] big data.[61] Individually

[51] Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 2017: 37.
[52] Daniel Kreiss, 'Prototype Politics: Technology-Intensive Campaigning And The Data Of Democracy' *Oxford University Press* (2016).
[53] *ibid.*
[54] Rasmus Kleis Nielsen, *Ground Wars* (Princeton University Press 2012).
[55] Carole Cadwalladr, 2018.
[56] Jamie Doward and Alice Gibbs, 2017.
[57] Carole Cadwalladr, 2018.
[58] "Donald Trump's campaign demonstrated to the whole world the potential offered by a mass analysis of individual data generated by the traces of our online activities, especially in social media. The development of social media and the illusionary anonymity they offer allowed scattered information about us to be collected." Piotr Pawelczyk, Jakub Jakubowski and Przeglad Politologiczny, 2017: 37.
[59] April Glaser, 2017.
[60] Upturn, 'Data Brokers In An Open Society' (Open Society Foundations 2016).
[61] "Massive amounts of personal data are gathered without a pre-established goal Bart van der Sloot, 'How To Assess Privacy Violations In The Age Of Big Data? Analysing The Three Different Tests Developed By The Ecthr And Adding For A Fourth One' (2015) 24 Information & Communications Technology Law: 74-103.

examined the data on voters seems irrelevant but, when collected and analysed it displays regularities and makes it possible to design a highly precise profile of relatively small groups. Such dynamic was empowered by social media capacity to collect and process massive amounts of scattered data and make inferences on its basis.

Big data grants the possibility to determine, for instance, political opinions on voters, relying on demographic, geographic, psychographic or behavioural aspects, to do it. Such aspects can be easily found on social media, where our names and age are displayed, as well as other personal information that is made available by the users. This makes it possible for data analytics, by means of algorithms that collect scattered data and do an automated analysis, to correlate the information and detect political preferences or behavioural characteristics. Thus, it is possible to widely target the electorate with adverts tailored to their characteristics.

The wide scale of this phenomenon is mainly driven by web user's inclination to publicize a vast amount of personal data or their ignorance about how to use the web safely,[62] even though the processing of data by third parties can be due to various reasons. The data industry benefits nowadays, not only of quantity and quality of digitally recorded data but, also of facilitated access to, storage, analysis, and sharing of this information coupled with increasingly advanced analytical techniques.[63]

Nevertheless, it is the people's endless web browsing on both, mobile and desktop devices that allows for the tracking of such information by interested third parties.[64] Particularly, the constant use of mobile devices enhances the mentioned vast publication of data, which constitutes a valuable source of revealing data (e.g. location, the apps they used, and their contacts)[65] that allows for a simplified access and subsequent processing of data by third parties "like Google and

[62] "Many data brokers collect and organize data that is available to the general public. Data brokers will commonly collect such data using "web crawlers" (software programs designed to automatically collect data from the Internet) or purchase it from other data brokers that specialize in digitizing particular types of records. Publicly available data includes (…) Media, social network and online data, including public information from LinkedIn, Facebook, Twitter, and Youtube and discussion sites." In Upturn, 2016: 10.
[63] Upturn, 2016: 6.
[64] "A visit to a single website will often trigger interactions with dozens of other organizations involved in advertising or analytics, many of which either are data brokers or exchange data with brokers" In Upturn, 2016: 6.
[65] *ibid.*

Apple or app developers and the data brokers that provide developers with analytics and advertising".[66]

Irrespectively of what makes this phenomenon possible, the novelty around the individualization on political campaigning and its surprising level of detail, made possible by algorithms, is worth to outline as a new trend. Parties are now appealing narrowly to their base of supporters through the accurate platforms provided by technology.

After a two decades trend of personalization in political campaigns, in all likelihood, data and analytics, which make the communication with the electorate intensively more efficient, will be a prominent subject and practice in the following years.[67] Therefore, an effort to precisely describe the process behind the developing micro-targeting techniques must be made.

2.3.1. Political micro-targeting

A variety of practices to monitor and profile the electorate, techniques of direct marketing to poll, canvass and get-out-the-vote are used nowadays as campaign basis,[68] to efficiently "activate the base, persuade undecided voters, and improve partisan turnout".[69]

One of the most newsworthy[70] practices emerges in the context of political communication of the *new technology-intensive era*[71] namely, political micro-targeting.[72] Political micro-targeting consists in "'creating finely honed messages targeted at narrow categories of voters' based on data analysis 'garnered from individuals' demographic characteristics and consumer and lifestyle habits'[73]".[74] However, this practice may be materialized in different techniques. It may consist in a form of political direct marketing, allowing parties, through predictive modelling techniques, to

[66] Upturn, 2016: 6.
[67] Even though this model of campaign is applicable only to quite a limited extent of parties, those with the capability to invest in it. Furthermore, the usage of such techniques will also depend on the amount of supporters and funding provided to the parties as well as the responsiveness of the electorate to the techniques.
[68] Colin Bennett, 2016: 261-275.
[69] Ira Rubinstein, 2014: 882.
[70] Carole Cadwalladr, 2018.
[71] Daniel Kreiss, 2016.
[72] Ira Rubinstein, 2014: 882.
[73] William A. Gorton, 'Manipulating Citizens: How Political Campaigns' Use Of Behavioral Social Science Harms Democracy' (2016) 38 New Political Science: 62.
[74] Frederik Borgesius and others, 2018.

divide potential voters into small groups according to their political preferences and then target them accordingly with their needs and interests - sending one message to one group and a different, even contradictory, message to another, while ignoring others. Yet, political micro-targeting may also consist in political behavioural advertising,[75] a technique[76] involving "tracking people's online behaviour to use the collected information to display individually targeted advertisements".[77]

Numerous approaches to 'micro-targeting' are distinguished other than the mentioned namely, geographical targeting[78] and demographical targeting,[79] which are also often used in 'micro-targeting' depending on the goal to achieve.[80]

The described techniques, represent partially the change from creating a message for mass audiences to tailoring messages accordingly to target a categorised audience.[81] In sophisticated political campaigns these techniques are usually algorithm based,[82] which identifies the electorate 'key' characteristics to subsequently target them with personalised messages[83] from the political party.

Considering the described techniques, it can be claimed that micro-targeting and modelling techniques are related. Even though there is not a direct correlation between both techniques, since 'micro-targeting' is possible without modelling, here I will focus on modelling considering the opinion that 'data becomes meaningful only through voter modelling'.[84] Modelling is what makes the new forms of political engagement move, 'distilling hundreds of data points into simple

[75]Joseph Turow, *The Daily You: How The New Advertising Industry Is Defining Your Identity And Your Worth* (2011); Frederik J. Zuiderveen Borgesius, 'Improving Privacy Protection In The Area Of Behavioural Targeting' [2015] SSRN Electronic Journal.
[76] This techniques makes use of a behavioural targeting approach, processing data on the voter's individual attitudes, behavior and values.
[77] Frederik Borgesius and others, 2018: 3.
[78] Its analysis is based in precinct-level results from past elections to identify promising electoral constituencies.
[79] Demographic characteristics, for instance, income religion or occupation are used to target groups which share such individualities.
[80] Simon Kruschinski and Andre Haller, 2018.
[81] Colin J. Bennett, 2014.
[82] Simon Kruschinski and Andre Haller, 2018.
[83] Carole Cadwalladr, 2018.
[84] Daniel Kreiss, 2012: 71.

categories of voters: likely supporters, those that can be persuaded, and those supporting another candidate'.[85]

Modelling is "the practice of using algorithms and observed data to build statistical or machine learning models to mine users with similar attitudes and behaviours (clustering) or predict unobserved actions or preferences (predictive modelling)".[86] Rubinstein,[87] separates predictive modelling work in three main steps:

1- Collection of voter's data like voter history, party registration, age, gender, income and race, as well as up-to-date response data (that might reveal partisan interest) by an analytic team;
2- Correlations and patterns generated by linking the above-mentioned characteristics established by statistical experts, through algorithms, to obtain the electorate categories;
3- Application of the predictive model to the electorate to achieve the likelihood of supporting the specific party.

In light of the above, data modelling is considered a decisive technique to enable political micro-targeting to effectively occur. Nonetheless, there are essential 'tools' complementary to voter modelling that need to be shown in order to understand how political micro-targeting functions.

2.3.1.1. 'Crucial tools' to political micro-targeting

Kreiss[88] considers it is the connection of massive amounts of data into categories of voters, through voter modelling[89] that transformed data into a crucial tool to political parties. The connection that makes it possible to categorize the electorate into potential supporters of the party

[85] Daniel Kreiss, 2012: 71.
[86] Simon Kruschinski and Andre Haller, 2018.
[87] Ira Rubinstein, 2014: 882.
[88] Daniel Kreiss, 2012.
[89] As described in the previous paragraph. See above 2.3.1.

or not, so the resources of the candidate are effectively used to target the electorate. Such connection is obtained through profiling.

Profiling is as a group of characteristics, features and attributes with each a person or a group is separated from another.[90] Technically, and considering automated-based profiling in this context, profiling is the outcome of data mining.[91]

The massive amounts of data available today make data mining a referenced statistical technique to substantiate a hypothesis and to clarify assumptions, using statistical methods that split the relevant and non-relevant correlations. Data mining enables the interested parties to get a prediction based on the data previously collected and analysed. Significant unforeseen correlations in data and subsequently patterns, generate a hypothesis, a prediction.

2.4. Risk assessment of political micro-targeting techniques

Political micro-targeting involves a panoply of risks, the majority of which are intimately connected with the stage of profiling although it is not limited to that phase of the process. The main risks identified are the following: *dataveillance*, normalisation, customization, and loss of privacy, equality and fairness.[92]

Firstly, *dataveillance* pertains to data surveillance which means that data controllers can collect, aggregate and store data on citizens that, most likely, they made available, direct or indirectly. Subsequently the same processed data can be integrated in other databases, mined or sold to other parties.[93] Ultimately, the one's that possess data on citizens can access and explore the opportunities provided by the data, predicting the future behaviour of citizens, for instance. Still, Solove[94] rejects the threat that the "Big Brother is watching you", often associated to the said

[90] Paul De Hert and Hans Lammerant, *Predictive Profiling And Its Legal Limits: Effectiveness Gone Forever* (Amsterdam University Press/WRR 2016).
[91] The use of algorithms so patterns of correlations between data are found in large databases gathered form different sources. In Mireille Hildebrandt, 'Defining Profiling: A New Type Of Knowledge?', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010) (2): 17-46.
[92] Mireille Hildebrandt, 2010 (1): 305.
[93] Mireille Hildebrandt, 2010 (1): 305-306.
[94] Daniel J Solove, *The Digital Person. Technology And Privacy In The Information Age* (New York University Press 2004).

endless data surveillance, and considers that *dataveillance* is not the biggest concern regarding profiling of citizens, an opinion I humbly agree with. However, I personally think the commercial interests of third parties in people's data should not be diminished and that the effect of the data surveillance should be weighted in the long term[95] since, the profiles will be stored and may be used at any time to target people for the third parties own benefit.

As regards to the use of the citizen's personal data in the future, a *normalisation* risk stands out. Normalisation is described as the effect of utilization of the data, gathered at any time, to anticipate behaviour and change the citizen's habits to fit the expectations of third parties. "When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? (…) profiles will begin to normalize population from which the norm is drawn', according to Lessig".[96] Pursuant this affirmation, it is feared that from the anticipation of people's behaviour, actual manipulation and subsequent change of that behaviour follows, which could result in the normalisation of the population behaviour according to the categorisation assigned to each person.

Furthermore, it is argued that apart from being constantly 'watched', people might be watched without noticing it, raising a concern on transparency of data processing. Such suspicion although evident for some, is confirmed today to the public in the field of politics, thanks to the 'Cambridge Analytica' case.[97] The case clearly showed not only that 'micro-targeting' is a political campaigning technique occurring in Europe but, most importantly that personal data on voters is being processed behind their back. In Cristopher Wylie's words political micro-targeting constitutes "a 'gross unethical experience', because you are playing with the psychology of an entire country, without their consent or awareness and not only are you doing that but you are doing it in the context of the democratic process",[98] statement pursuant to which I have to agree with. Even though an ethical analysis is outside the scope of this thesis, legally speaking, all personal data processing needs a set of interlinked obligations and rights for transparency,[99] which are being undermined. This is only aggravated in a democratic system that is characterised by

[95] Mireille Hildebrandt, 2010 (1): 306.
[96] Mireille Hildebrandt, 2010 (1): 307.
[97] See bellow paragraph 2.5.3.2.
[98] The Guardian, 'What Is The Cambridge Analytica Scandal?' <https://www.youtube.com/watch?v=Q91nvbJSmS4> accessed 25 March 2018.
[99] Upturn, 2016.

people's political freedom to choose that may be severely hampered due to the secrecy embed in such campaigning techniques, which can be used to manipulate people's choice.

In line with the above and also incompatible with democracy is life *customisation* that arises due to *filtering* – 'the process that enables us to filter incoming noise and information in order to receive only the information we appreciate'.[100] It is implied that in a democracy people should be confronted with all kinds of information, not tailored to a specific type of personality or political preference, that is to say, the opposite that stems from filtering. Also, citizens should have common experiences in a diverse society. In a society where people live more and more through virtual networks, depriving the population from unique and differentiated experiences online, might endanger the electorate's freedom to form an opinion and choose, subsequently hampering the democratic process.

Moreover, risks on privacy and security arise from the possibility of data breaches or the dissemination of sensitive citizen information,[101][102] endangered when stored for a long period of time, especially if held by political parties which are in constant campaign.[103] Also, a privacy and data protection concern emerges from the poor access and lack of control of our own personal information. "What data is processed?", "what knowledge is built with the data on citizens?", "(…) by which organizations?" are common questions to which an answer is not given explicitly.[104] Again, fear over the opacity that encircles political micro-targeting are on spot and raise concerns over *fairness* and *equality* in its non-discriminatory[105] dimension. Fairness concerns mainly the shift in power balance between political parties that are able to 'micro-target' citizens and the electorate that is targeted even though, without any control or knowledge on how their data is processed and for which purposes.[106] The relationship between political parties and voters is illustrative of an unwanted but clear information asymmetry between the two concerned parties.[107] As regards to equality, there is a risk of the materialisation of discriminatory practices concerning

[100] Mireille Hildebrandt, 2010 (1): 307.
[101] E.g. race, gender, political opinion, etc.
[102] Daniel Kreiss, 2012: 73.
[103] Constant campaigning includes frequent changes in staff, candidates and leaders, which in this scenario constitutes different parties that might have access to the data stored in different periods of time.
[104] Mireille Hildebrandt, 2010 (1): 309.
[105] Article 21 of the Charter of Fundamental Rights of the European Union (2000/C 364/01).
[106] Mireille Hildebrandt, 2010 (1): 309.
[107] *ibid.*

data processing due to the information unevenness that arise from profiling techniques, that basically choose what information different 'types' of citizens have access to, according to their singular characteristics (e.g. race, gender, etc.).

In the political context[108] the fear of such risks materializing intensifies since variables such as political competitiveness, discourse and representation are added. However, one may ask if there is a reason to fear the manifestation of such risks throughout Europe since until recently, political micro-targeting and its associated effects where only firmly entrenched and discussed in-depth in North America. Therefore, in order to keep up with the technological advancements in the field of politics and with the possible necessity of further prevention of such risks in mind, the deemed presence of political micro-targeting practices in Europe must be investigated.

2.5. How such tendencies are being imported to Europe

The culture and the different political institutions of each country play an imperative role when examining whether new practices based on data analytics will be accepted or not.[109] The political culture in the United States has been an influencing factor along the years, for the development of practices of monitoring and targeting of the electorate.[110] The tolerance to political micro-targeting techniques was highly induced in the U.S. not only because of the cultural "fever" for elections but also due to a soft legal framework regarding privacy.[111] The practices adopted in the U.S. elections revolve around a liberal campaign finance system, a First Amendment that provides protection for political speech, a singular election structure that focuses on two dominant political parties, a powerful political consulting industry, a digital economy and culture that puts huge emphasis on the power of Big Data. Nevertheless, most importantly, the U.S. political party's benefit from a weak and fragmented privacy legal framework, being the voter intelligence data considered "the largest concentration of unregulated personal data in the US today".[112]

In contrast, the European political culture exhibits a general distrust upon intrusive political marketing and campaigning techniques as such, supported by a strict privacy and data protection

[108] Daniel Kreiss, 2012: 73.
[109] Nick Anstead, 2017: 294-313.
[110] Colin J. Bennett, 2016: 262-264.
[111] *ibid*.
[112] Ira Rubinstein, 2014: 882.

framework.[113] However, data-driven politics has been influencing the political campaigning process in some European countries, creating a prospect of dissemination of these practices through Europe namely, in The Netherlands, Germany and the UK.

So, given the existence of enlightening case studies in the mentioned countries confirming the presence of political micro-targeting in the European political campaigning practices, the following paragraphs of this thesis will address not only the strong manifestation of this practice through Europe but also, the different ways in which such campaigning practices manifest themselves consonant the culture and political scenario of each country. Consequently, bearing in mind the risks surrounding 'micro-targeting' it is important to discuss the European practices to establish the state of play.

2.5.1. The Netherlands

Some scholars used the 2017 elections in the Netherlands as a case study[114] to find out how and to what extent campaigns in a European multiparty democracy, use political behavioural targeting techniques.

Although some disparities between parties were found, it was concluded that all campaigns have used political behavioural targeting through Facebook and some parties even developed their own tools.[115]

> "Some campaigns also employ 'dark posts', a Facebook function that enables campaigns to opaquely target specific audiences, while its messages are not visible to untargeted Facebook users. Campaign leader 1 exemplifies:
>
> "We've managed to get something done related to gas extraction in Groningen. It doesn't make sense to share that on the national Facebook page, because it was only important news locally. So we put out a dark post, only for Groningen residents. Sometimes we can specify it even more" In Tom Dobber and others, 2017.

[113] Colin J. Bennett, 2016: 262-264.
[114] Tom Dobber and others, 2017.
[115] Tom Dobber and others, 2017: 12-13.

The above-mentioned case study managed to show, with a real-life example, how behavioural targeting can be useful in a Parliamentary system and highlights how these techniques are able to put smaller parties in the spotlight in such a way that would be impossible with traditional media, fostering a fair dissemination of information in the campaigning process. Although the budget of parties is not considered a constraint to the adoption of political behavioural targeting tools, the GDPR might be.[116] Plus, in most European countries the electoral register is inaccessible to political parties, contrarily to what happens in the U.S., therefore the access to data is highly restricted. Nonetheless, the study states that although different, both the political and legal systems[117] do not bar the use of the political behavioural targeting, considering Facebook as a communication enabler.[118]

In short, the 2017 elections in the Netherlands showed that on one hand the impact of technology in politics can be positive, considering smaller parties may more easily reach the public through social media, on the other hand, I do not believe that they will be able to reach voters with the same speed and scope as the 'big' parties do. Nonetheless, while it constitutes an advantage for all political parties, social media might not come as an advantage for the electorate. As the case study shows, campaigns "opaquely target specific audiences" with dark posts via Facebook, evidently undermining one of the core principles surrounding the processing of personal data, the principle of transparency. Thus, it seems evident that the constraints imposed by the GDPR assume greater importance, especially regarding to the enforcement of the controller's transparency obligations towards the electorate. Therefore, even if the technological advancements may assure good sources of information for the electorate to consult, in case of using targeting processes, it is imperative that political parties are clear, transparent and legitimised by those concerned to safeguard the self-determination of each of the targeted voters.

2.5.2. Germany

Traditionally, political campaigning in Germany occurs through door-to-door canvassing. Such method allows parties to collect voter information without undermining the strict privacy

[116] Colin J. Bennett, 2016: 261–275.
[117] E.g. inaccessibility to the electoral registry and more strict data protection legislation in Europe.
[118] Tom Dobber and others, 2017: 10; 17.

laws, which forbids candidates from collecting personal data on voters without their consent.[119] Therefore, canvassers are collecting information on the electorate through the "Connect17 app" linked to an exact GPS coordinate. However, the party is not allowed to record voter's names and addresses,[120] making the data only valuable to target people at their homes, contrarily to the practices in the U.S. that reach e-mails or telephones.

> "Golembiewski gives a CDU pamphlet to a woman at her home near Jena's main train station and talks to her about the party's goals, just like in any other election season. But what is different this time around is that once she closes the door, he pulls out his smartphone and opens an app called Connect17. First, he clicks on a smiley face to show that the conversation went well and then enters the woman's estimated age, gender and any questions she had about the campaign. (The woman will then have to confirm that she's willing before the data actually gets registered.) When he clicks the last button, he wins 100 points, which will increase his ranking among fellow canvassers.
> The Connect17 app has been audited in the German state of Saarland, and Praxisnah, the company that developed it, made a few adjustments to comply fully with privacy laws." In DW (www.dw.com), 'CDU, SPD And Greens Use Big Data To Target Bundestag Voters | DW | 26.08.2017' (*DW.COM*, 2018) <http://www.dw.com/en/cdu-spd-and-greens-use-big-data-to-target-bundestag-voters/a-40244410> accessed 23 May 2018.

Kruschinsky and Haller state in their study that data-driven canvassing as used in Germany's political campaigns cannot be compared to the mechanisms used in the U.S.[121] The study shows that only geographical targeting based on the analysis of precinct-level results from past elections, is used to identify auspicious electoral constituencies for their canvassing efforts. The micro-targeting as it is used in the U.S. would be extremely restricted by privacy laws, political and cultural factors, since not only the information on voter's party preferences and records of

[119] The Economist, 'Campaigning In Germany' (2017) <https://www.economist.com/news/europe/21728994-new-technology-has-brought-door-door-campaigning-continental-europe-campaigning-germany> accessed 18 May 2018.
[120] The party can only build files on general locations and geographical regions rather than individual voters.
[121] Simon Kruschinski and Andre Haller, 2018.

participation are unavailable, but also such techniques are considered offensive to Germans, reminding of an unwelcome history of overbearing government.[122]

Though this is not the case study that best describes the central issue of this thesis, it is still worthy of great thoughtfulness considering it is illustrative not only of the presence of the technological developments in European campaigns but also, and most importantly, of how the culture and political history of a country impacts the implementation of such developments, which were expressed in different targeting approaches. In contrast with the previous case study, in Germany there was not an obvious infringement of data protection rules and regulations, at least concerning lawfulness or transparency of processing. However, it does not cease to be a geographical targeting case that may carry as much risks as the infamous cases of behavioural targeting. In this case too, the characteristics of each voter are gauged, and inferences are made from them for campaigning purposes, although with the voter consent. At bottom, targeting can be manifested in various approaches but, the correspondent future harmful risks remain.

2.5.3. The UK

2.5.3.1. The 2015 general election

The first reported case of data-driven politics in the U.K. concerned the 2015 general election. According to a study on the data-based campaign techniques used in the election,[123] a data-driven targeting strategy was adopted and considered decisive for the victory of the Conservative party.

The case study in which this analysis is based,[124] raises some cultural and political concerns, since not every political party in the UK can support such forms of campaigning. The

[122] Ruth Marcus, 'Germany'S Throwback Campaign' *The Washington Post* (2013) <https://www.washingtonpost.com/opinions/ruth-marcus-germanys-throwback-campaign/2013/09/24/14043b4e-2540-11e3-ad0d-b7c8d2a594b9_story.html?noredirect=on&utm_term=.85aa8883ca2c> accessed 18 May 2018.
[123] Nick Anstead, 2017.
[124] *ibid*.

unequal opportunities between parties are especially evidenced in the access to voter's data, area in which the smaller parties have limited resources, as shown:[125]

> "The role of polls in data-gathering is complex, meaning that terminology needs to be clearly demarked, differentiating public polls, large sample polls, and surveys. For smaller parties, notably UKIP, but also the Liberal Democrats, public polls (…) allowed them to decide which constituencies they might be viable in and to target resources accordingly (…). Larger parties were able to conduct their own polling, either with large samples or focused on key constituencies (…). Research at this scale is obviously very expensive."

The study reiterates that the Conservative campaign was the most effective by adopting the recent U.S. innovation of targeting individual voters. Even though, it is claimed that the Labour party also sustains a data-driven campaign and that it is assisted by a formidable staff and number of supporters.[126] Nevertheless, it still uses segment-based targeting, making its efforts less targeted, and therefore less effective. Moreover, such statements confirm our opinion already expressed in the first case regarding the 2017 elections in the Netherlands, with regard to the thought that the economical differences between political parties are not a constraint when reaching voters through data-driven targeting techniques. Nevertheless, even the parties which lack such resources, the smaller parties, are benefiting from the "boom" of 'Big Data' although with less far-reaching means.[127]

[125] Nick Anstead, 2017.
[126] *ibid.*
[127] The use of smartphone applications propagated by the Liberal Democrats are a great example of it. In Nick Anstead, 2017.

Furthermore, the 2016 Vote Leave campaign, illustrates another occurrence[128] of data-driven politics. According to an LsE Project,[129] the Vote Leave campaign invested into digital advertising to explore their resources more effectively. So, The director of campaign Dominic Cummings explained:[130]

> "In the official 10-week campaign we served about one billion targeted digital adverts, mostly via Facebook and strongly weighted to the period around postal voting and the last 10 days of the campaign. We ran many different versions of ads, tested them, dropped the less effective and reinforced the most effective in a constant iterative process".

However, little was known regarding the scale and the functioning of such techniques or its influence on the electorate or in the ballot results, at least until March 2018, when the 'Cambridge Analytica' files on Brexit were revealed:[131]

> "The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box."

[128] Jamie Doward and Alice Gibbs, 2017.
[129] Emma Goodman and others, 'The New Political Campaigning' (he London School of Economics and Political Science 2017).
[130] Emma Goodman and others, 2017.
[131] Carole Cadwalladr, 2018.

2.5.3.2. 'The Cambridge Analytica files'

'Cambridge Analytica', the data analytics firm in the focus of the media headlines[132][133][134][135] all over the world is a data marketing firm established in the market of Big Data and Psychographics.[136] Its activity involves the harvesting of data online with the aim of creating 'micro-targeted' content, tailored to the characteristics found in the analysis of the data collected on users. Accordingly, it is now known that the company offered its services to Trump's and Vote Leave campaign.

The data analytics firm "uses data to change audience behaviour"[137] and to this end, since 2014, Facebook became the main source from which data would be collected and used for private commercial purposes not considered or authorized by the users, "to build a system that could profile individual US voters, to target them with personalized political advertisements".[138] The logic behind the described system was achieved years earlier when a paper in the Proceedings of the National Academy of Sciences journal (2013) showed that profiles made on (what is considered) insignificant data such as, random 'likes' were able to reveal unexpected and intricate individualities usually invisible to the human eye.[139] The possibility to infer and predict the individual's most complex attributes from their digital information was shown by the paper as well as its capacity of application to a large spectrum of the population without them being aware of what was happening. This discovery meant that "commercial companies, governmental institutions, or even your Facebook friends could use software to infer attributes such as

[132] Carole Cadwalladr, 2018.
[133] Alana Abramson, 'Cambridge Analytica Whistleblower Tells U.K. Lawmakers His Predecessor Was Poisoned' [2018] *TIME* <http://time.com/5216680/cambridge-analytica-christopher-wylie-predecessor-poisoned/> accessed 10 April 2018.
[134] Craig Timberg and Karla Adam, 'Christopher Wylie: How Cambridge Analytica's Whistleblower Became Facebook's Unlikely Enemy' *Independent* (2018) <https://www.independent.co.uk/news/long_reads/christopher-wylie-cambridge-analytica-facebook-data-breach-whistleblower-trump-election-a8267991.html> accessed 10 April 2018.
[135] Channel 4 News, 'Revealed: Trump'S Election Consultants Filmed Saying They Use Bribes And Sex Workers To Entrap Politicians' <https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation> accessed 18 May 2018.
[136] Concordia, 'Cambridge Analytica - The Power Of Big Data And Psychographics' <https://www.youtube.com/watch?v=n8Dd5aVXLCc>.
[137] *The Guardian*, accessed 25 March 2018.
[138] Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[139] "When users liked "curly fries" and Sephora cosmetics, this was said to give clues to intelligence; Hello Kitty likes indicated political views; "Being confused after waking up from naps" was linked to sexuality." In Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).

intelligence, sexual orientation or political views that an individual may not have intended to share.",[140] and that is exactly what 'Cambridge Analytica' did. The data analytics firm seized the opportunity and secretly, away from the public scrutiny, engaged in these practices. However, thanks to Cristopher Wylie the subject is on 'today's' agenda and the way the citizens data was processed by the company is exposed and submitted to the public scrutiny.[141]

In the ex-employee of 'Cambridge Analytica' words: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on."[142] Such declarations are based on fresh revealed documents by the observer, proving the harvesting of massive amounts of data and the consequent knowledge of Facebook in the matter. The documents unveil the process used in the campaigns, being clearly explained that after gathering data on thousands of voters through a personality app developed by the academic Aleksandr Kogan,[143] even though for academic instead of commercial purposes, an algorithm was built and used to identify likely political persuasions and personality individualities so, the firm could apply the so called 'micro-targeting' technique, designing specific messages that were likely to appeal to the categories of individuals.[144]

To enable the 'micro-targeting' process, massive amounts of data were collected via the 'thisisyourdigitallife' app. The app collected not only data on the app user's but also, on the user's entire friend network,[145] leading to the rapid expansion and accumulation of data on most of the voters, even if the users had no idea of such consequences. Subsequently, information available on the voter's Facebook profile susceptible of revealing personal individualities was harvested.[146] The harvested data generated in turn, thousands of profiles that could be matched to electoral

[140] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).
[141] Carole Cadwalladr, 2018.
[142] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).
[143] Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[144] The Guardian, 'The Brexit Whistleblower: 'Not Cheating Is The Core Of What It Means To Be British' <https://www.youtube.com/watch?v=7vo1u9JRZG8&index=4&list=PLa_1MA_DEorHSyKo2uelblYGZLP6e4Cyg>.
[145] In The Guardian, 'What Is The Cambridge Analytica Scandal?' <https://www.youtube.com/watch?v=Q91nvbJSmS4&index=2&list=PLa_1MA_DEorHSyKo2uelblYGZLP6e4Cyg>.
[146] E.g. status updates, likes and in some cases private messages. In Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).

roles,[147] which would then be sold and used to build the algorithm capable of processing the data previously gathered.[148] The apparently insignificant data harvested becomes significant quickly when investigated through an algorithm revealing of the most intimate details. A user's sexual orientation, race, gender, prediction of the most susceptible party to support and even intelligence or childhood trauma can be revealed through the algorithm developed by 'Cambridge Analytica', without the need to go deep into personal messages or status updates although that was done.[149]

In so doing, the revealing data on the electorate was processed and turned into an invisible but powerful campaign weapon, able to reach all voters personally according not only to their susceptibility to accept the message but also through the design of the most receptive frames of advertisement.

> "Instead of standing in the public square and saying what you think and letting people come and listen to you and have that shared experience (…) you are whispering into the ear of each and every voter and you are maybe whispering one thing to this voter and another thing to another voter. We risk fragmenting society in a way where we don't have more shared experiences and we have no more shared understanding. If we don't have more shared understanding, how can we be a functioning society?" In The Guardian, 'Cambridge Analytica Whistleblower: 'We Spent $1M Harvesting Millions Of Facebook Profiles' <https://www.youtube.com/watch?time_continue=4&v=FXdYSQ6nu-M> accessed 23 May 2018.

Both cases in the UK, regarding the 2015 general election and the Vote Leave campaign are demonstrative of the rapid and uncontrolled development of technology in the field of politics throughought Europe. As previously noted in the Netherlands case, not only the legitimacy to access personal data on voters is undermined, as regards to the unknown purposes for which data are collected, but also, the transparency of the whole process, which is significantly desired when the processing of personal data is at stake.

[147] Carole Cadwalladr and Emma Graham-Harrison, 2018 (1).
[148] *ibid.*
[149] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).

The UK cases illustrate a reality where the users of social media had no idea their data was pulled or how it was pulled and, above all, how it was used. Such scenario is mostly explanatory of various issues but, most importantly, paves the way for the subject discussed in this thesis, the opacity surrounding political micro-targeting.

2.6. Conclusion

In contrast with the U.S., where political micro-targeting is deemed as a common practice, the European political culture exhibits a general distrust upon intrusive political campaigning campaigning techniques as such, supported by a strict privacy and data protection framework. This tendency implied a few years ago that advanced political marketing techniques would not thrive in Europe. However, nowadays case studies have shown that data-driven politics has entered the realm of political campaigning in some European countries, creating a prospect of dissemination of these practices through Europe.

The analysis of the case studies on elections in the Netherlands, Germany, and especially the UK concerning the 'Cambridge Analytica' case, brings to light an issue that no longer is only theoretical but perpetuate on citizen's lives. Today, it is proven that political parties are 'micro-targeting voters'. Political parties are targeting the electorate with advertisements fitting their type of personality on the basis of profiles. These profiles are made, mainly based on Facebook data, without the public knowing data are being processed on them for commercial purposes, let alone that data on their friend network is being affected by processing data for the same purposes. In the end, as the case demonstrates, the electorate has no clue how political micro-targeting is developed or even if it is being developed. Questions like 'who has been targeted?', 'why a specific person was targeted?', 'which processes are used?' are some of the main questions illustrative of a huge transparency issue in political micro-targeting.

However, the GDPR establishes requirements to ensure a fair and transparent processing of personal data. Therefore, in the next chapter I will focus on the transparency obligations related to political micro-targeting under the GDPR.

3. Political micro-targeting and the Data Protection Framework

3.1. The European Data Protection Framework

Profiling is perceived to be a reality as old as life, as a 'kind of knowledge that unconsciously or consciously supports the behaviour of living beings'.[150] Profiling techniques generate knowledge, representative of correlations made from past actions that posteriorly enable a more or less accurate prediction of future behaviour. These predictions might then be used to target individuals in specific scenarios – political campaigns, respectively. Gutwirth and De Hert[151] affirm that "profiles are patterns obtained from a probabilistic analysis of data; they do not describe reality". Therefore, deemed as a common and vague 'exercise', profiling is reckoned as legitimate even though it is agreed that transparency rules may be observed in principle, to enhance visibility, controllability and accountability of profilers as well as information control of the individuals concerned.[152]

As demonstrated in the previous chapter, the reality of profiling has somewhat changed and nowadays it benefits from a high level of accuracy in its effects, propitiated by precise algorithms.[153] The massive amounts of data available on individuals staunch in online platforms allows not only to deduce behavioural characteristics of individuals with a fair amount of precision but in certain cases it allows for algorithms to manipulate their behaviour through 'micro-targeting'. However, the processing of personal data involved in these techniques is often invisible to the data subject, therefore, concerns in ensuring transparency of the processing of personal information must be take into account with regard to the obligations and correspondent rights established under the GDPR.

[150] Serge Gutwirth and Paul De Hert, 'Regulating Profiling In A Democratic Constitutional State', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010): 290.
[151] Serge Gutwirth and Paul De Hert, 2010: 289.
[152] *ibid.*
[153] Maja Brkan, 'Do Algorithms Rule The World? Algorithmic Decision-Making In The Framework Of The GDPR And Beyond' [2017] SSRN Electronic Journal.

According to the concepts used in the GDPR, political micro-targeting is based on profiling as defined in its article 4 (4).[154] Hence, profiling may involve solely automated decision-making, meaning not only the general provisions on the GDPR but also the specific article 22 of the GDPR applies to the data processing, or not, case regarding which only the general provisions on data processing involving profiling are applicable.[155]

In particular, considering the GDPR requirements as well as the A29WP Guidelines,[156] it is assumed for this thesis development that political micro-targeting qualifies as automated decision-making for the purposes of Article 22 of the GDPR. Even though it is believed that cases of targeted advertising usually do not fulfill the needed requirement of having a 'significant effect on the individual'[157], it is still recognized that online advertisements may have a 'significant effect on the individual' depending on the context in which the targeting occurs. Thus, considering the characteristics and factors underlying each case[158] , in the end "the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned."[159]

Political micro-targeting, as it was revealed by the previously referred cases,[160] decides on which individual to target with political party's advertisement, based solely on the results provided by an algorithm that constructs on citizens (illegitimately obtained) profiles revealing of the personalities more susceptible to certain kinds of messages and ideas as well as political preferences or other interests of the voter, with the aim to change the electorate's behaviour and subsequently, affect the electorate supposedly free choice – fact that was shown by psychological studies, supportive of the mechanism as well as by the latest developments in politics.[161]

---

[154] "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;" See article 4 (4) of the GDPR.

[155] Ira S. Rubinstein, 'Big Data: The End Of Privacy Or A New Beginning?' (2013) 3 International Data Privacy Law: 79.

[156] Article 29 Data Protection Working Party (17/EN WP 251), 2017.

[157] Article 29 Data Protection Working Party (17/EN WP 251), 2017.

[158] The following characteristics shall be considered on a case by case basis: (a) the intrusiveness of the profiling process; (b) the expectations and wishes of the individual concerned; (c) the way the advert is delivered; and (d) the particular vulnerabilities of the individuals targeted. See Article 29 Data Protection Working Party (17/EN WP 251), 2017.

[159] Article 29 Data Protection Working Party (17/EN WP 251), 2017.

[160] See above paragraph 2.5.

[161] 'In addition to having data scientists and psychologists and strategists, they also have an entire team of creators, designers, videographers, photographers. They create that content that then gets sent to a targeting team which then injects it into the Internet. Websites will be created, blogs will be created, whatever is that we think this target profile will be receptive to, we will create content on the internet for them to find and then they see that, they click and they

Accordingly, it is acknowledged that the voting rights of the electorate can be affected significantly[162] where political micro-targeting is based on behavioural profiling, qualifying it as automated decision-making for data protection purposes under the GDPR requirements. Consequently, not only article 22 of the GDPR will be applicable but also the general provisions on profiling with emphasis on the transparency concerns referred in the recital 71 of the GDPR.[163]

Pursuant the Regulation, the political micro-targeting technique, dependent on the collection and analysis of personal data, although not explicitly forbidden,[164] is subject to transparency obligations[165] to not only guarantee the rights of data subjects, especially when sensitive data is involved,[166] but also to ensure the accountability to whom it may concern.

In addition to the processing of personal data on the electorate, political micro-targeting is increasingly reliant on algorithms, as a form of enhancing the party's decision-making. These algorithms are the foundation of the 'micro-targeting' effectiveness by determining the information that must be received by each individual. However, those constitute an indecipherable tool to the public, which is demonstrative of the opacity of 'micro-targeting' along with the fact that the public is not aware that such processing takes place. Accordingly, the accountability of the entities using 'micro-targeting', will likely prove highly difficult, what is particularly worrying since the technique might carry a risky impact for the population, that does not know on which variables the decisions to 'micro-target' are taken, let alone strive to claim their own rights.

---

go down the rabbit whole (…) until they start to think something differently.' In The Guardian, 'What Is The Cambridge Analytica Scandal?' <https://www.youtube.com/watch?v=Q91nvbJSmS4&index=2&list=PLa_1MA_DEorHSyKo2uelblYGZLP6e4Cyg>.

[162] 'Explanatory Text For Proposal For A Council Directive Concerning The Protection Of Individuals In Relation To The Processing Of Personal Data, COM (90) 314 Final – SYN 281': .29.

[163] "In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions." In recital 71 of the GDPR.

[164] Articles 22 and 9 of the GDPR and recital 56 of the GDPR.

[165] Article 5 (4) of the GDPR.

[166] E.g. race, gender, political opinion.

The enactment of a stricter Regulation to new forms of political campaigning might be challenging, due to the massive collection and processing of data traces on the individual,[167] but in legal terms, no profiling is done separately from data protection legislation,[168] meaning the processing of data occurring must comply with the rules laid down in the GDPR.

Thus, I believe that the analysis of the principle of transparency according to the European data protection legislation, is the boiling point when considering political micro-targeting. The strict data protection framework of the GDPR might inhibit the use by political parties of profiling techniques and subsequently decision-making, preventing them to categorize, assess and discriminate between people.[169] Therefore, the transparency requirements associated to the techniques used in political micro-targeting need to be clarified and the standards set by the data protection legislation need to be meet to avoid the risks posed by new forms of political campaigning.

As stated by the Electronic Privacy Information Center (EPIC) in an attempt to call on algorithmic transparency, "voters should "know as much about advertisers as advertisers know about voters."".[170] Therefore, the purpose of this chapter is to enlighten the electorate on the transparency obligations of controllers when processing personal data, established in the GDPR. To make a concrete analysis I am going to construct on the 'Cambridge Analytica' case and apply the transparency principle specifically regarding the circumstance in that case.

3.2. A need for transparency

Apart from the opacity surrounding political micro-targeting, one of the biggest concerns is also equality in its non-discriminatory[171] dimension with regard to informational content asymmetries.[172] Epistemological flaws and biases may be a consequence of data-driven practices,

[167] Article 29 Data Protection Working Party, 'Guidelines On Automated Individual Decision-Making And Profiling For The Purposes Of Regulation 2016/679 (17/EN WP 251)' (European Commission 2017).
[168] Serge Gutwirth and Paul De Hert, 2010: 271-302.
[169] Isak Mendoza and Lee A. Bygrave, 'The Right Not To Be Subject To Automated Decisions Based On Profiling' [2017] EU Internet Law: 77-98.
[170] Electronic Privacy Information Center, 'EPIC - EPIC Promotes 'Algorithmic Transparency' For Political Ads' (2017) https://epic.org/2017/11/epic-promotes-algorithmic-tran-1.html.
[171] Article 21 of the Charter of Fundamental Rights of the European Union (2000/C 364/01).
[172] See above paragraph 2.4.

which means that 'micro-targeting' may lead to results biased by the information harvested or even by the code embodied in the algorithms.[173] Also, political micro-targeting may produce not only unfair and unequal outcomes, but may also be considered an intrusive practice to one's (subject to the decisions) autonomy, if the behaviour and consequently the freedom of choice of the voter is undermined. Still, the consequences of political micro-targeting may be daunting but without knowledge over the features that underlie the decision-making embed in 'micro-targeting', it is impossible to assess if the process is deceptive, discriminatory or unethical.

The possibility of manipulation of the accessibility to knowledge in secrecy, make individuals vulnerable to abuse from data analytics firms and incapable of appealing against unlawful or unfair results that may occur.[174] Therefore, a necessity to empower the electorate against data analytics firms and political parties campaigning tools arise, in order to avoid such disastrous consequences and hold accountable the concerned parties that might infringe rights and freedoms of the electorate. But, how can the electorate hold the parties accountable when they do not even know political micro-targeting takes place?

Ideally, the premise that "observation produces insights which create the knowledge required to govern and hold systems accountable",[175] is the logic behind transparency. Accordingly, the more we know about a system's inner workings, for instance the more transparent the 'micro-targeting' process is, more defensibly the system can be governed and the concerned parties held accountable.[176] However, transparency is not just "a precise end state in which everything is clear and apparent,"[177] but implies knowledge over what is observed so, only in that case transparency promises a form of control by the one's claiming their rights.[178] Hence, transparency is obtained as long as the information given to the public is visible, discernible and understandable, making the system's inner workings clear to the concerned parties.

[173] Emre Bayamlloolu, 'Transparency Of Automated Decisions In The GDPR: An Attempt For Systemisation' [2018] SSRN Electronic Journal: 17.
[174] Emre Bayamlloolu, 2018: 17.
[175] Mike Ananny and Kate Crawford, 'Seeing Without Knowing: Limitations Of The Transparency Ideal And Its Application To Algorithmic Accountability' (2016) 20 New Media & Society: 974.
[176] *ibid.*
[177] *ibid.*
[178] Mike Ananny and Kate Crawford, 2016: 975.

Transparency creates a promise of openness, accountability and autonomy, creating the subsequent prospect of making easier to regulate behavior of the actors in a democratic society.[179]

Therefore, to promote compliance of the parties involved in data analytics in politics, the obligations that are imposed by in the article 5 of the GDPR must be considered, namely the transparency obligations, as a promise of openness to the electorate, accountability of the parties involved and autonomy of the users.

It may not be certain that transparency will eradicate every risk to the citizen's associated with political micro-targeting however, I believe it is a good place to start, bearing in mind its stance as a core principle concomitant to the processing of personal data and the promise of giving at least some control to the electorate over the data that is processed on them. Only the processing of data that is transparent allows for the exercise of the data subject's rights and freedoms.

3.3. The principle of transparency

The principle on transparency of processing is enshrined in article 5 (1) (a) of the GDPR and it reads as follows:

"*1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'),*"[180]

To the processing of personal data to be lawful, fair and transparent it is important that the individual knows and understands how his/her personal data is being utilised.[181][182] To this end, the transparency principle embodied in the article 5 of the GDPR needs to be emphasised as a significant value to guarantee the clarity that should be provided to data subjects with regard to the personal data processed on them – "*It should be transparent to natural persons that personal data*

[179] Mike Ananny and Kate Crawford, 2016: 975.
[180] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[181] Recital 39 of the GDPR
[182] Paul Voigt and Axel Bussche, 'The EU General Data Protection Regulation (GDPR): A Practical Guide' [2017] Springer International Publishing: 88.

concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed".[183]

The principle of transparency concerns:[184]

- "Information to the data subjects on the identity of the controller"[185];
- Information to the data subjects on the purposes of the processing;
- "Further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed"[186];
- Making natural persons aware of risks, rules, safeguards and rights[187] in relation to the processing of personal data and how to exercise their rights in relation to such processing.

Also, it is ideal that at the time the personal data is collected, the purposes for processing personal data are determined as well as explicit and legitimate.[188]

To comply with the transparency obligations, the information given to the data subject should be intelligible, that is to say, easily accessible and understandable for the data subject in question, through the use of clear and plain language.[189][190]

The automated decision-making including profiling practices, are usually invisible to the human eye as well as complex, reason why the GDPR established specifically article 12 (1), according to which "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form,*

[183] Recital 39 of the GDPR.
[184] *ibid.*
[185] *ibid.*
[186] Recital 39 of the GDPR.
[187] Articles 13 and 14 of the GDPR.
[188] Paul Voigt and Axel Bussche, 2017: 88.
[189] Recitals 39 and 58 of the GDPR.
[190] "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used." In recital 58 of the GDPR.

using clear and plain language…".[191][192] So, it is the controller's obligation to guarantee that all the relevant information on the processing of personal data[193] is provided to the data subject, given the potential risks of profiling.[194]

The risks of unfairness and inequality are a constant to profiling. [195] Such risks can be materialized in examples such as: denying people access to employment opportunities, or in our case, manipulating the access to information which is tailored to the specific and intimate characteristics and interests in the political micro-targeting process. Therefore, not only it is important that the controllers or data analytics firms take the appropriate measures that the GDPR requires them so the data subjects are aware that the creation of personalised profiles and its utilisation by political parties are a possibility; as well as what and how those methods create and use such profiles.[196] Additionally, it is required that the information provided to the users is presented in an intelligible way, so the 'micro-targeting' process is easily understandable but, most importantly, so users are truly informed and empowered with rights they can uphold.[197]

3.4. The singularities of algorithmic decision-making

Increasingly, automated decision-making becomes a reality in politics and with-it transparency becomes more difficult to guarantee, mostly given to the omnipresent technology developments – e.g. the technical and complex algorithms embed in 'micro-targeting'. Although algorithms might be effective and precise tools, their complexity makes them hardly explainable

[191] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[192] For data collected directly from the data subject this should be provided at the time of collection (Article 13); for indirectly obtained data the information should be provided within the timescales set out in Article 14(3).
[193] E.g. information about the collected data, and, if appropriate, the existence of automated decision-making referred to in Article 22(1) and (4), the logic involved, and the significance and envisaged consequences of such processing.
[194] Recital 71 of the GDPR.
[195] See above paragraph 2.4.
[196] Simone Van der Hof and Corien Prins, 'Personalisation And Its Influence On Identities, Behaviour And Social Values', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010): 119.
[197] "Users should also be informed of ways to access, review and update personal data and profiles and of the security of this process. Moreover users should know whether and how (e.g., by sending an e-mail to a clearly specified address) they can restrict or object to (commercial) use of their personal other data as well as whole profiles. In the case of web services, for instance, a privacy statement on the website of the service provider is a good instrument to provide such information. Privacy statements should be complete and easy to access and understand". *ibid*.

by the specialists or comprehensible towards the public. Consequently, decision-making based on algorithms will be considered opaque, due to both technical and social reasons.

If the citizen's do not know or understand the factors underlying the automated decision-making, the assessment of negative effects like, deceptiveness, discrimination or ethics violations in the process becomes impossible. The lack of perception of the process by the population exponentially increases the risks associated with automated decision-making practices and enhances the so called "functionality creep"[198] – the personal data that is processed for different purposes than the primarily established.[199]

Thus, a need for algorithmic transparency arises[200] regarding algorithmic-based decisions. Algorithmic transparency strives for "openness about the purpose, structure and underlying actions of the algorithms used to search for, process and deliver information".[201]

Moreover, algorithmic transparency constitutes a crucial approach to not only prevent negative effects such as, discrimination, but also to determine accountability in automated decision-making.[202] Even if the algorithms are not programmed to lead to discriminative results, algorithmic based decisions usually carry the risk to be discriminatory.[203]

Algorithmic-based decisions may turn out to be discriminatory due to biased entry datasets[204] or biased programming of the algorithm.[205] Therefore, algorithmic transparency may be enlightening towards the understanding of the reasons behind biased decision-making and would consequently be primordial towards preventing algorithmic discrimination, for instance.

In the case of 'Cambridge Analytica', data on race, gender or even sexual orientation that were collected to 'micro-target' the electorate,[206] is an example of a data input that may facilitate the materialisation of the risk of discrimination regarding the knowledge generated for each category of voter's. Additionally, the citizens in the UK were not aware nor had they given their

[198] Simone Van der Hof and Corien Prins, 2010: 119.
[199] Article 5 (1) (c) of the GDPR.
[200] Electronic Privacy Information Center, 2017.
[201] 'What Is Algorithmic Transparency? - Definition From Whatis.Com' (*SearchEnterpriseAI*, 2018) <https://searchenterpriseai.techtarget.com/definition/algorithmic-transparency>.
[202] Maja Brkan, 2017: 18.
[203] See above paragraph 2.4.
[204] When the data input is discriminatory (e.g. when special categories of data are involved in the decision-making for instance, data on race or gender of the individual).
[205] Maja Brkan, 2017: 18.
[206] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).

consent to political micro-targeting practices to be carried out[207] (even though suspicions were raised regarding the Vote Leave campaign itself),[208] let alone worry over possible discriminatory practices. These facts are illustrative of a huge transparency deficiency, principle that must be complied with when processing personal data, especially if it involves sensitive data. In this regard 'Cambridge Analytica', a Chair of the Article 29 WP reacted "As a rule personal data cannot be used without full transparency on how it is used and with whom it is shared. This is therefore a very serious allegation with far-reaching consequences for data protection rights of individuals and the democratic process. (…)".[209]

3.5. Conclusion

Political micro-targeting is a process usually shrouded in secrecy, subsequently raising concerns on opacity and unintelligibility as well as on the ruthless outcomes it may take namely, discrimination and manipulation of access to knowledge subsequently translated in the manipulation of the voter's opinion. In consideration of this transparency vulnerability, the obligations that are imposed in the article 5 (1) (a) of the GDPR to controllers must be considered so as to guarantee clarity of processing to data subjects.

A transparency need only intensifies when considering automated decision-making processes such as political micro-targeting, usually invisible to the public as well as complex, reason why the GDPR established additional transparency obligations for the controller in article 12 (1). It is the controller's obligation to guarantee that all the relevant information on the processing of personal data is provided "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*" to the data subject, given the potential risks of profiling (e.g. unfairness and inequality).

The mentioned risks are only intensified by omnipresent technology developments such as, the technical and complex algorithms embed in 'micro-targeting'. Its characteristics makes them hardly explainable by the specialists or comprehensible towards the public, consubstantiating

[207] The Guardian, 'What Is The Cambridge Analytica Scandal?', 2018.
[208] Jamie Doward and Alice Gibbs, 2017.
[209] Chair of the Article 29 Working Party, 'Cambridge Analytica – Reaction' (2018).

in the opaqueness of the decision-making. Hence, if the population does not know or understand the factors underlying the automated decision-making, the assessment of negative effects on the public becomes impossible. Thus, a need for algorithmic transparency arises regarding algorithmic-based decisions not only to prevent the micro-targeting effects but also to determine the distribution of accountability in automated decision-making.

Bearing in mind this need for transparency, and the evidence in the 'Cambridge Analytica' case that the obligations established for the controllers under the GDPR are not being complied with, one might question how the data subject will uphold this principle.

The data subjects should be informed of data processing activities concerning themselves to ensure the compliance with the transparency principle but most of all, to permit them to effectively exercise their rights in relation to the processing of their personal data. Therefore, in the next chapter I intend to analyse possible safeguards to ensure the transparency of automated decision-making including profiling under the GDPR as well as its adequacy and efficacy in protecting the electorate right to data protection.

4. Transparency in contemporary political campaigning: the electorate warranties

4.1. The data subject rights: the transparency warranties

The data subjects should be informed of data processing activities concerning themselves in order to comply with the transparency obligations and most of all, to permit them to effectively exercise their rights[210] in relation to such processing.[211] Only aware of the data processing, an individual can control how the personal data is used. Thus, the principle of transparency[212] must be the foundation of the information rights and correspondent obligations.

The obligations of transparency established for controllers[213] must be the building blocks of the communication with the data subject.[214] So, recital 71 of the GDPR states as follows: *"In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."*[215]

So, to comply with the transparency obligations, the controller must provide "(…) information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language, about any operation or set of operations on their personal data".[216] The way data is processed must be sufficiently comprehensible to fulfil the purpose of exercising the rights of the individual, according to the GDPR. Data processing is only transparent as soon as its comprehension is achievable.

The 'Cambridge Analytica' case proved how vulnerable the population is to the processing of personal data, and consequently to the possibly harmful risks of political micro-targeting.

Even though political micro-targeting is deemed legitimate, as automated decision-making,

[210] Paul Voigt and Axel Bussche, 2017: 141.
[211] Recital 39 of the GDPR.
[212] Article 5 (1) (a) of the GDPR.
[213] Article 12 of the GDPR.
[214] Paul Voigt and Axel Bussche, 2017: 142.
[215] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[216] *ibid*.

it is dependable on the implementation of measures under the GDPR. The Regulation binds data controllers to the implementation of suitable measures and safeguards in order to properly inform data subjects, to help them to protect their fundamental right to data protection. So, the data subjects are *"not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her",*[217] for instance.

Therefore, the rights established in the articles 13 to 15 of the GDPR namely, the right to be informed of the data processing and the right to access of the data subject are the foundation of individual's safeguards regarding automated decision-making including profiling. Hence, a descriptive and critical analysis of the rights embodied in the articles 13 to 15 of the GDPR will follow.

Also, even though the mentioned rights may be useful tools, its adequacy and effectiveness as remedies to ensure transparency is questioned and posteriorly scrutinized in this chapter.

4.2. Right to be informed

"*The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes*".[218] Thus, the controller is obliged to provide minimum information regarding data processing to the data subject before carrying out any processing activities.[219] Where data is obtained from another source, it is stated in article 14 (3) of the GDPR that the information shall be provided by the controller to the data subject within a reasonable period, after obtaining the personal data, but at the latest within one month, depending on the circumstances of the case. This obligation exists whether the personal data is directly collected from the data subject or from a different source.[220].

Additionally, under articles 13 (2) or 14 (2) of the GDPR, the controller shall provide the data subject with the additional information necessary to guarantee the transparency of processing, according to the specific circumstances and context in which the personal data is processed.[221] The

[217] Article 22 (1) of the GDPR.
[218] Recital 60 of the GDPR.
[219] Articles 13 (1) and 14 (1) of the GDPR.
[220] However, between those two cases, the minimum content of the information to the data subject slightly differs. In this regard, the general communication requirements under article 12 of the GDPR must be fulfilled.
[221] Recital 60 of the GDPR.

additional information strives to balance the informational intrinsic imbalance existent between the controller and the data subject, therefore, the provision must be deemed generally necessary and for that reason, mandatory.[222]

While the 'micro-targeting' technic and its inherent processes are usually shrouded in secrecy, the data subject should be informed of its existence and consequences.[223] Therefore, the right to be informed is the first step to answer the issue of political micro-targeting, involving the voter's personal data, currently clandestinely collected through a Facebook app without the data subject consent for further processing for commercial purposes or the data's subject's entire friend network endorsement.[224][225]

Considering the importance of the transparency principle[226] regarding profiling techniques involved in 'micro-targeting', the articles 13 (2) (f)[227] and 14 (2) (g)[228] of the GDPR, reads as follows:

"(...), the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[229]

Controllers are responsible for providing the specificities of the profiling techniques involved to reach a decision such as: (i) the engagement of the data subject in the process, (ii) the essential information on the logic involved and (iii) the significance and consequences of the data processing.[230]

[222] Paul Voigt and Axel Bussche, 2017: 145.
[223] Recital 60 of the GDPR.
[224] Carole Cadwalladr and Emma Graham-Harrison, 2018 (2).
[225] See above paragraph 2.5.3.2.
[226] Recital 60 of the GDPR.
[227] Concerns only data obtained from the data subject.
[228] Concerns only data not directly obtained from the data subject.
[229] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[230] Article 29 Data Protection Working Party (17/EN WP 251), 2017.

Even though establishing its existence may be easy, the profiling techniques involved in a specific type of processing can be intricate for the average person to understand. The acknowledgement of the logic of automated decision-making may be difficult to a data subject or even to the controller in some cases, especially concerning algorithmic-base decisions. For that reason, the controller must develop a simple and clear method to communicate to the data subject the rationale and the method of the processing behind decisions. The information provided has to be meaningful, which suggests that the data subject should be aware not only of the data involved in the processing, but also of the data that was inferred from it and led to the decision.[231]

In addition, pursuant to articles 13 (3) and 14 (4) of the GDPR, where the controller intends to process the personal data for a purpose different than the initial purpose for the data processing, the information on that purpose as well as other necessary information must be provided by the controller.[232]

Only in the cases stated in articles 13 (4) and 14 (5) of the GDPR the controller is under no information obligation. However, the latter is not considered to apply to the political micro-targeting cases presented on this thesis.

The information obligations established in the GDPR are, in my opinion, logical considering the course of action of the data subject depends on how much the individual knows about the data processing. If normally the relation between the data subject and the controller is uneven, in cases of automated decision-making, the need for balance is even bigger. The necessity to comply with the transparency obligations is even more pressing in complex mechanisms such as algorithm-based decisions embodied in 'micro-targeting'. The difficulty of the data subjects in enforcing their rights without information breeds the urgent need for compliance with such obligations.

Even though the existence of automated based-decisions inherently impose disadvantageous terms on the data subjects in all branches, the politics branch is particularly

[231] Article 29 Data Protection Working Party. (2017). *Guidelines on Automated Individual decision-making and profiling for the purposes of Regulation 2016/679* (17/EN WP 251). Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm.

[232] "In order to prevent additional expenses at the occasion of such change of purpose, controllers should try to communicate predictable, future purposes of processing to the data subjects upon collection of the data." In Voigt, P., Bussche, & A. (2017). *The EU general data protection regulation (GDPR): A practical guide*. Cham: Springer International Publishin. P.145.

worrying. In the case of political micro-targeting, the electorate, knows nothing, neither such data processing takes place nor how it happens or what are its consequences. Therefore, the implementation of information obligations will involve some effort of the controllers to achieve actual compliance. An end has to be put to the secrecy stigma involved in political micro-targeting, evasive of the data subject's rights.

4.3. Right of access or a right to an explanation?

The right of access by the data subjects to their personal data constitutes another way to increase fairness and transparency of data processing. It ensures that data subjects verify the lawfulness of data processing activities and that their rights under the GDPR are enforceable.[233]

Different then the right to be informed,[234] the right of access shall go beyond providing the general information on data processing activities to the data subjects. So, more in-depth information shall be given to the data subject to meet its objective of guaranteeing the lawfulness of data processing.

The article 15 (1) (h) of the GDPR states the following:

"*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information…"*[235]

Contrarily to the right to be informed which has to be proactively fulfilled by the controller, to exercise the right of access an action is required from the data subject; a request for information.

The right indicated in article 15 of the GDPR involves two steps.[236] First, the data subject "shall have the right to obtain confirmation from the controller" [237] as to whether or not his/her

[233] Recital 63 of the GDPR.
[234] Articles 13 and 14 of the GDPR.
[235] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[236] Paul Voigt and Axel Bussche, 2017: 150.
[237] Article 15 (1) of the GDPR.

personal data is being processed. Then if the data processing is confirmed, the data subject shall have access to "the personal data and the following information" [238] processed on them, as catalogued in article 15 (1) of the GDPR. This approach sounds simple, however, in practice it is difficult for the controller to properly respond to those 'steps'.

The exercise of the right of access depends on a request from the data subject. So, the response of the controller to the requests made under article 15 of the GDPR are constrained by the data subject request for information. An appropriate way to handle the request will depend on its scope, if it is limited to a confirmation that the processing takes place, or whether it involves exhaustive information on processing.[239]

Generally, regarding profiling, the provision provides the data subject with the right to obtain, from the controller, not only the inferred personal data but also the categories of data used in the adopted profiling technique.[240]

To ensure a lawful processing of personal data, under article 15 of the GDPR, the exercise of the right to access shall be "simplified".[241] Accordingly, the information provided pursuant the data subject's request must be concise, transparent, intelligible and easily accessible, supported by the use of clear and plain language and not later than 1 month after receipt of the request.

Pursuant article 15 (3) of the GDPR the controller shall provide a copy of the undergoing processing of personal data to the involved data subject. Additionally, article 15 of the GDPR must comply with the general requirements established under article 12 of the GDPR.[242]

The right to access should not adversely affect the rights or freedoms of others, according to article 15 (4) of the GDPR, which include trade secrets and intellectual property rights, in

[238] Article 15 (1) of the GDPR.
[239] Paul Voigt and Axel Bussche, 2017: 151.
[240] Article 29 Data Protection Working Party (17/EN WP 251), 2017.
[241] Recital 63 of the GDPR.
[242] This entails, among others, that the first copy shall be provided to the data subject free of charge (article 12 (5) of the GDPR). Where the controller processes a large quantity of information concerning the data subject, the controller should request that, before information is delivered, the data subject must specify to which information or processing activities its request relates (Recital 63 of the GDPR). Upon reversion, if the data subject wishes to obtain information on all processing activities carried out by the controller and such request does not qualify as excessive, the controller has to provide comprehensive information to the data subject in question.

particular copyright protecting software.[243][244] However, the provision should not be used as a refusal to provide all information to the data subject.[245]

On automated decision-making, including profiling, article 15 (1) (h) of the GDPR reads as follows:

"(…)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[246]

The provision provides the data subject with the right to obtain, from the controller, the same information that can be requested under Articles 13 (2) (f) and 14 (2) (g) of the GDPR - the existence of automated decision making, including profiling, meaningful information about the logic involved and the significance and envisaged consequences of such processing for the data subject, respectively.

Nonetheless, some authors find that this provision useful not only for the individuals to access their data but also to provide them, in a more direct way, a transparent explanation. This is so because it is believed that the information left to be given, after an individual exercise the right to be informed, will only concern the general "system functionality" of the algorithm, and the data inferred from it. In other words, it concerns the data that arouse from the automated decision-making, the "after processing". Edwards and Veale[247] think that Article 15 might comprise a wide right to an explanation extended to all forms of automated decision-making.[248] Conversely, according to other authors the existence of the so-called 'right to explanation' remains

[243] Recital 63 of the GDPR.
[244] "This includes potential effects of the copy on personal data of others that might become relevant when information is provided by controllers that are subject to professional secrecy, such as lawyers whose documentation is likely to contain information on the opposing party of their client." In Paul Voigt and Axel Bussche, 2017: 153.
[245] Recital 63 of the GDPR.
[246] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[247] Lilian Edwards and Michael Veale, 'Slave To The Algorithm? Why A Right To Explanationn Is Probably Not The Remedy You Are Looking For' [2017] SSRN Electronic Journal: 53 (1).
[248] Even though it has been suggested that Article 15 (h) is restricted like Article 22 of the GDPR.

questionable,[249] being even considered non-existent but rather what some called a "limited right to be informed".[250]

According to the Article 29 WP, the information provided under article 15 of the GDPR should concern the "*envisaged consequences* of the processing, rather than an explanation of a *particular* decision".[251] Such affirmation is clarified in recital 63, according to which every data subject should have the right to know and obtain 'communication' about automatic data processing,[252] including the logic involved, and *at least* when based on profiling, the consequences of such processing. Consequently, the data subject can be aware of the logic of the decision made concerning his/her data. So, the information provided to the data subject should contain the factors taken into account for the decision-making process, and their respective 'weight' on an aggregate level, so the data subject has enough information to examine the lawfulness of the decision-making and hence challenge the decision.

Within this framework of thought, although the referenced authors[253][254][255] disagree with regard to the existence of a right to explanation under article 15 of the GDPR, even the ones that assume its existence, tend to doubt of the feasibility of a 'right to explanation' of automated decisions.

Ideally, the right to explanation is a promising mechanism to ensure accountability and transparency in, artificial intelligence, robotics, automated systems and algorithmic based decisions.[256] Again, ideally, an instructive right to explanation would require data controllers to explain how the decision-making is processed in the technologies, empowering data subjects into exercising their given rights and posteriorly foster accountability of third parties of which data processing should become completely transparent, to the extent allowed by law.[257] However, the provision containing the possibly right to explanation as defined under the GDPR, is considered

[249] Maja Brkan, 2017.
[250] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why A Right To Explanation Of Automated Decision-Making Does Not Exist In The General Data Protection Regulation' (2017) 7 International Data Privacy Law: 76-99.
[251] Article 29 Data Protection Working Party (17/EN WP 251), 2017.
[252] "(…) In particular with regard to the purposes for which the personal data is processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.". In recital 63 of the GDPR.
[253] Lilian Edwards and Michael Veale, 2017: 53 (1).
[254] Maja Brkan, 2017.
[255] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 2017: 76-99.
[256] *ibid.*
[257] Lilian Edwards and Michael Veale, 2017: 53 (1).

unlikely to overcome the transparency barriers built-in algorithmic based decisions[258] due to a plethora of reasons.

First, the provision is considered restrictive, unclear or even paradoxical making the enforcement of a right to explanation unforeseeable.[259] To ensure legal certainty to the data subjects, the vocabulary, especially the core concepts used in the provisions must be precise and explicit, so no doubt remains on the safeguards provided against automated decision-making.[260] Ambiguous expressions such as "(…) significance . . . envisaged consequences . . . (…) logic involved"[261] must be explicit. Additionally, the right to explanation is constrained from the beginning by the restrictive definition of 'automated decision-making' in Article 22(1). Therefore, not only the vocabulary should be sharpened but clear requirements should be introduced to enlighten the data controller on his/her obligations.[262]

Second, the perception and understanding of the technicalities embodied in technology used for automated decision-making is usually difficult for the public due to, mainly, the complexity and opacity underlying algorithmic mechanisms as well as the lack of literacy regarding data analytics.[263] So, even if well-defined and intended, explaining algorithmic based-decisions can easily turn out to be uninformative, turning the right to contest a decision meaningless.[264]

The right to an explanation should enable the data subject to understand how a specific input turns into a certain output, to foresee the outcome of an automated decision and act upon the decision.[265] Moreover, the specific contexts and system have to be observed. An assessment of the feasibility of the right to obtain an explanation to fulfil the transparency principle has to be done on a case-by-case basis. Also, account should be taken of the fact that even when algorithmic models, inputs and weightings are revealed, discriminatory or unfair practices may not be

[258] Lilian Edwards and Michael Veale, 2017: 53 (1).
[259] *ibid.*
[260] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 2017: 76-99.
[261] Article 15 (1) (h) of the GDPR.
[262] "Evidence regarding the weighting of features, decision tree or classification structure, and general logic of the decision-making system may be sufficient. However, the risks for innovation and beneficial processing posed by a right to explanation that requires automated decision-making methods to be." In Emre Bayamlloolu, 2018.
[263] Emre Bayamlloolu, 2018.
[264] Lilian Edwards and Michael Veale, 2017: 53 (1).
[265] E.g. "in a predictive model for credit eligibility, providing customer with a decision tree or similar visualised form of the decisional model could be difficult to work out even for the highly educated citizens." In Emre Bayamlloolu, 2018.

perceptible. "Most algorithms will display inadvertent bias rather than explicitly coded-in bias: designers will not want to be sued or prosecuted for illegal action (…)".[266] So, the negative effects that stem from an algorithm may not be perceptible by an in-depth analysis of the input data and correspondent weightings, turning extremely difficult to protect the data subjects.

Hence, article 15 (1) (h) of the GDPR can be both, a useless or powerful instrument to data subjects depending on its future interpretation. The success of this mechanism will be greatly influenced by the interpretation of entities such as, the European Supervisory Authorities and the national courts.

Finally, as a violation of the data subject's right to access might entail considerable fines for the controller under article 83 (5) (b) of the GDPR, it should be ensured that such requests are processed and acted upon in a diligent manner. Companies should review available options for giving their access mechanisms a more transparent design and for introducing possible technical and organisational solutions.

4.4. The (in)adequacy and effectiveness of the remedies provided by the GDPR in the 'new world of politics'

In chapter 2 it was acknowledged that a multitude of possible harms are associated with political micro-targeting.[267] *Dataveillance*, normalization, customization and loss of privacy are examples of risks that cannot be ruled out. Nevertheless, the opacity of data processing and its correspondent consequences concerning the electorate's access to knowledge cannot be forgotten, considering the impact data protection has on political micro-targeting, due to imposing rights and obligations regarding transparency of processing.

At present, as defended by some authors[268] the GDPR does not guarantee transparent and accountable automated decision-making, at best information about the existence of automated decision-making and system functionality may be provided. Though the case studies earlier described,[269] demonstrate the opposite is happening regarding contemporary campaigning

[266] Lilian Edwards and Michael Veale, 'Enslaving The Algorithm: From A Right To An Explanationn To A Right To Better Decisions?' [2017] SSRN Electronic Journal: 1-15 (2).
[267] See above paragraph 2.4.
[268] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 2017: 76-99.
[269] See above paragraph 2.5.

practices. Therefore, the guarantees of the electorate against political micro-targeting, an algorithmic decision-based mechanism, are diminished and the risk that the electorate becomes more vulnerable to developing technologies grows due mainly to three specific and previously described reasons.

First of all, the core concepts enshrined in the provision are ambiguous and therefore, unreliable when it comes to guarantee the data subject right of access.

Second of all, revealing information about automated-decision making does not make data subjects understand how the decision came about because of the inherent complexity of the process.

Lastly, even if there is a possibility that information on the automated decision-making process is disclosed, the electorate has no insight into the actual practice of contemporary campaigning taking place. So, how should data subjects actively exercise their right of access to information, when they do not even know data is being processed?

Taking into account these considerations, in case the right of access turns into an empty formality',[270] measures urge to be taken to balance positions.

The information and access rights have emerged to address the challenge of transparency under the GDPR. However, while individual rights can be useful, the information and access rights entail only two of many solutions for the data subject to oversee the ongoing data processing and exercise the correspondent legitimate rights embodied in the Regulation. Although the importance of these rights to ensure transparency of data processing is not disregarded, giving the opportunity to the electorate to contest specific decisions, it is demonstrated above that the rights in question encompass serious practical and conceptual flaws.[271]

Furthermore, if on the one hand these rights may place undue burden on the data subject (in the case of the right of access where the initiative to require the information is of the data subject) on the other hand the power given to the controller may be excessive. Therefore, the effectiveness in ensuring transparency expected from such rights although possible, is not considered substantively helpful as currently framed in the GDPR. As long as the compliance with the right to information that enlightens on the existence of data processing depends on the controllers

[270] Lilian Edwards and Michael Veale, 2017: 7 (2).
[271] Lilian Edwards and Michael Veale, 2017: 1-15 (2).

initiative, not only the existence of the data processing cannot be guaranteed but the rights dependent on such information also cannot be secured, as is the case of the right of access.

Illustrative of the scenario described is political micro-targeting. As previously described,[272] political parties are usually interested in keeping their campaign strategies in secrecy from other party's but mostly from the electorate, especially when it involves data processing on them. The only certainty today, regarding the latter, is the one provided by Christopher Wylie, the whistleblower behind the 'Cambridge Analytica' case.[273] Consequently, if the controllers have no incentive to provide information on the existence of data processing and if the choice to provide such information is on their 'hands' only, it is deemed likely that transparency of processing keeps being undermined by campaigning interests of political parties. With regard to this, I hope the newly imposed administrative fines[274] in the GDPR create enough incentive for compliance with the informational obligations although preventive measures should be put in place simultaneously to effectively guarantee the controller complies with the respective obligations and rights of the electorate are secured.

Therefore, considering political campaigning techniques are increasingly and deliberately hidden from the data subject, it is concluded that the informational rights on the GDPR are a good start to ensure transparency of data processing however, not enough to effectively guarantee it.

4.5. Conclusion

Data subjects should be informed of data processing activities concerning themselves to ensure compliance with the transparency principle as set out in the GDPR, to permit them to effectively exercise their rights in relation to the data processing and consequently, to ensure accountability of the concerned parties.

With regard to the transparency obligations, the rights to be informed of the data processing and the right to access of the data subject are considered to be the foundation of the safeguards to automated decision-making including profiling. These rights assure the communication with the data subject, and for that reason these are the building blocks of transparency.

[272] See above paragraph 2.5.
[273] See above paragraph 2.5.
[274] Article 83 of the GDPR and recitals 148 to 152 of the GDPR.

Presently, however, it is considered that the both rights of the GDPR do not guarantee transparent automated decision-making since the warranties conceded to the data subjects under the GDPR are being firmly challenged in many circumstances. At best, the 'right to be informed' about the existence of automated decision-making and system functionality may be successfully granted if effectively enforced. However, the explanation aimed to be provided within the right of access faces a few obstacles. First, the core concepts in its provision are ambiguous and urge to be clarified by experts or jurisprudence. Second, the lack of awareness or understanding of the public regarding the technicalities of political micro-targeting holds back an effective enforcement of the right. Third, the obstacles are exacerbated if the right to information is not complied with in first place, as is often the case in political micro-targeting. Even if there is a possibility that information on the automated decision-making process is disclosed, the electorate has no insight into the actual practice of 'micro-targeting' taking place. Lastly, if the choice to provide such information is on the controllers 'hands' only, it is likely that transparency of processing keeps being undermined by campaigning interests of political parties. Therefore, the guarantees towards the electorate against political micro-targeting, an algorithmic decision-based mechanism, are diminished and as the electorate becomes more vulnerable concerning developing technologies, measures urge to be considered.

In view of the above, it is crucial to analyse the GDPR remaining mechanisms that may be able to guarantee the transparency of data processing, in the particular case of political micro-targeting. Therefore, using the GDPR as a basis, I intend to unravel possible solutions to answer the electorate transparency issue to improve their position in the democratic system.

5. Transparency in contemporary political campaigning: the electorate remaining possibilities

5.1. Political micro-targeting and the transparency challenge

The ambiguity of the provisions in the GDPR, the high complexity of algorithm-based decisions or the obvious secrecy behind such process, are the main obstacles to a proper enforcement of the transparency principle regarding political micro-targeting. Due to such conceptual and practical flaws[275] the voter's informational and access rights are being undermined and further mechanisms to avoid it must be explored.

It is crucial to analyse the GDPR remaining mechanisms that may be able to guarantee the transparency of data processing, in the particular case of political micro-targeting. Therefore, using the GDPR as a basis, I intend to unravel possible solutions to answer the electorate transparency issue, considering the automated decision-making informational deficiency, to subsequently improve their position in the democratic system, by guaranteeing their informational rights.

To conclude, an analysis will be carried out to carefully examine if the data protection fundamental right of the electorate, as specified in the GDPR, is safeguarded considering the opacity atmosphere surrounding political micro-targeting.

5.2. Data protection by design

Privacy by Design, known as "engineering as a way to build privacy-aware or privacy-friendly systems, generally voluntarily",[276] paved the way for what is today data protection by design (hereinafter, DPbD) as it is currently framed in the GDPR.[277] Essentially, privacy by design

[275] See more in the above paragraphs 4.2. and the following.
[276] Lilian Edwards and Michael Veale, 2017: 7 (2).
[277] Article 25 of the GDPR.

"is a process involving various technological and organizational components, which implement privacy and data protection principles."[278]

Yet, DPbD illustrates the emphasis on preventive data protection in the GDPR made as intended by the EU legislator. Accordingly, data protection principles such as, data minimization should be built into technology.[279]

Technological developments made their way into all areas of society, including politics. While political campaigning enjoys the perks of processing personal data, data protection needs to be effectively enforced by preventive protection measures and DPbD may be one of those. This comes from the line of thought that not everything can be regulated with a top-down approach, but that regulation should start in code, a bottom-up solution.[280]

Pursuant article 25 of the GDPR, in order to implement DPbD *"(...) the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures*". The suggestions of measures include pseudonymisation, "*designed to implement data-protection principles (...) in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*".[281] Essentially, it is encouraged that data protection is automatically enforced in information systems by the controller from the beginning of the processing operation.[282] Therefore, measures to comply with the transparency principle could be conceived into technology to prevent the secrecy of its existence and the probable irregular access to the individuals data from the beginning.

In the field of political micro-targeting where massive amounts of data are gathered daily to be built into profiles of voters, I strongly believe that the incorporation of such preventive measures into technology could ease the implementation and the compliance with the data protection principles while enhancing the protection of the electorates' data from an early stage, preventing it from further abuse by political parties, whose power would be limited from the start.

---

[278] ENISA, 'Privacy and Data Protection by Design – from policy to engineering' [2014]: 3. file:///C:/Users/u512671/Downloads/Privacy%20and%20Data%20Protection%20by%20Design.p df.
[279] Paul Voigt and Axel Bussche, 2017: 62.
[280] *ibid*.
[281] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[282] Bert-Jaap Koops and Ronald Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology: 161.

In this regard, specific measures concerning DPbD will be proposed to address the transparency issue contemporary to political micro-targeting in the final chapter on 'Recommendations'. [283]

5.3. Data protection impact assessments (DPIA)

A DPIA consists in the assessment of the impact of data processing in specific contexts with the purpose of demonstrating suitable measures to address those to comply with the GDPR.[284] Hence, it is an important tool of the accountability principle under the GDPR.[285] Article 35 (1) of the GDPR states as follows: *"Where a type of processing in particular using new technologies(...) is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data"*[286].

The purpose of DPIAs are not to stop the data processing, but to provide counter measures for future operations of systems that may carry a high risk to the data subjects.

Article 35 (3) (a) of the GDPR requires that a DPIA is carried out if "*a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*"[287]. So, if a system based solely on automated decision-making involving the data subject's profiles has a high impact on them and it cannot depend on the individual's consent, on a contract with the individual or on a law authorising this, the controller must carry out a DPIA primarily to data processing.[288]

Thus, a DPIA could be advantageous in identifying measures to address the transparency issues involved in the data processing such as the high risk of "use of inferred data and predictive

[283] See below paragraph 6.2. for specific recommendations on DPbD measures.
[284] Article 29 Data Protection Working Party (17/EN WP 251), 2017.
[285] Article 5 (2) of the GDPR.
[286] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[287] Retrieved from REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.
[288] Lilian Edwards and Michael Veale, 2017: 1-15 (2).

analytics"[289] where sensitive personal data[290] is processed on a "large scale", of which 'micro-targeting' is an example.

Also, when the DPIA indicates high risks on the specific data processing, the controller must consult a DPA prior to processing"[291] so, measures to mitigate the high risks involved in processing are conceived. Thus, the consultation of a DPA can function as another tool to enhance transparency since the data processing happening in the political context of campaigning would have to be brought to the authority's attention.

Overall, DPIAs may foster better systems for data processing due to not only enhancing the protection of the electorate rights by raising red flags but also to bring awareness of the use of personal data to the authorities[292] and consequently, the public. It must be emphasized however, that DPIAs cannot replace the information and access rights role. First, because DPIAs are not targeted directly to users, but to builders and regulators.[293] Second, because DPIAs are not imperatively public documents.

In short, the public acknowledgement of algorithm-based decisions is not sufficiently ensured by such mechanism. DPIAs raise important concerns regarding the impact on the citizens' rights and freedoms but in practice they are not aimed to solve them.

5.4. Certification systems

The GDPR introduces, for the first time in the European Law, a certification mechanism, enshrined in articles 44 and 43. Certification is an inherently flexible concept so, a variety of definitions are established by different authors.[294] It can be defined as an assessment procedure for conformity, while some authors define it as a "voluntary conformity assessment procedure carried out by an external and accredited auditor on the basis of requirements published by a recognized

[289] Information Commissioner's Office (ICO), 'Big Data, Artificial Intelligence, Machine Learning And Data Protection': 71.
[290] E.g. race, gender or political opinion.
[291] Article 36 (1) of the GDPR.
[292] Recital 94 of the GDPR.
[293] Lilian Edwards and Michael Veale, 2017: 1-15 (2).
[294] Eric Lachaud, 'Quelle Peut Tre La Contribution De La Certification La Protection Des Donnnes Personnelles? (What Can Be The Contribution Of Certification To The Data Protection?)' [2017] SSRN Electronic Journal.

authority",[295] a management system or as "a trademark protecting the rights of third parties who have been authorized to use that mark".[296]

The certification system constitutes a tool for accountability since it is a method according to which the controller may report compliance with the GDPR.

The drafting of a certification reference system is encouraged by the European Commission in the GDPR considering the benefits that it may implicate for the data subjects.[297] Certification seeks to ensure a high level of security of data processing, which may be achieved through the certification of technologies protective of data.[298]

For the data subjects, certification is not only a synonym of security but also a way to ensure transparency. Certification, when achieved and published, ensures transparency of the data processing of the entity in question, making it easier for individuals to scrutinize relevant data practices and correspondent consequences.[299] Most importantly, the certified processing of personal data will be considered public knowledge so the citizens can actually know the processing is taking place, constituting a great step towards enhancing transparency of processing.

Specifically, article 42 of the GDPR suggests voluntary[300] certification of controllers and processors to reveal compliance with the Regulation, through the development of "certification mechanisms" and "seals and marks". Considering this provision together with article 43 of the GDPR, in the particular scenario of political micro-targeting as an algorithm-based decision system, two ways to operationalize certification to two main aspects of algorithmic systems may be developed so transparency is enhanced posteriorly.[301]

It is proposed that the algorithm is certified as a "software object" by directly specifying either its design specifications or the process of its design, such as the expertise involved"[302] and

[295] "Certification is the (voluntary) assessment and approval by an (accredited) party on an (accredited) standard" In Gabriele Jahn, Matthias Schramm and Achim Spiller, 'The Reliability Of Certification: Quality Labels As A Consumer Policy Tool' (2005) 28 Journal of Consumer Policy: 57.
[296] Eric Lachaud, 2017.
[297] Article 42 (1) of the GDPR.
[298] Eric Lachaud, 2017.
[299] Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).
[300] Article 42 (3) of the GDPR.
[301] Lilian Edwards and Michael Veale, 2017: 7 (2).
[302] *ibid*.

that the output-related requirements of an algorithm, that can be monitored and evaluated, are specified. Also, it is suggested that the entities involved in data processing or even the process using the system to make decisions, which would consider algorithms as situated in the context of their use, are certified.[303]

On the one hand the mentioned proposals could institute important tools to enhance transparency. On the other hand, reliability, efficacy and accessibility are crucial concerns, considering the trends in the privacy domain of self-regulation of the private sector by seal and certificates.

Firstly, the certification procedure is antagonistic in its basis, in a private sector scenario at least, since the candidate to the procedure is also a customer.[304] So, the certification body finds itself in predicament where it must not only maintain a demanding and impartial procedure that ensures quality of the certification but also should satisfy its clients, so they keep interested in the service provided by the certification authority.[305] The more the certifier discovers fraud, the more its quality is legitimised however, the clients may lose interest in the services.

Secondly, even if the algorithms are certified, their functioning might not be intelligible to the public;[306] also, the effects of algorithmic decision-making are difficult to prevent or explain since negative effects for the data subjects do not necessarily derive from the input data on its basis, it is unpredictable from where such effects come from.[307] Therefore, it seems difficult to calculate the effectiveness of certification in enhancing the transparency of political micro-targeting as it is difficult to measure the algorithm indicators.

Thirdly, an accessibility issue arises with regard to the levels of services of high quality of services developing countries in comparison to the advantaged developed countries which have a clear advantage towards obtaining certification to its services.[308] Such characteristic will most

[303] Lilian Edwards and Michael Veale, 2017: 7 (2).
[304] Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).
[305] *ibid.*
[306] See above paragraphs 3.4. and 4.3.
[307] See above paragraphs 3.4 and 4.3.
[308] Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).

likely contradict the requirement established in article 42 (1) of the GDPR in its terms since, small and medium-sized enterprises are not sufficiently taken into account regarding the *ratio* of the certification systems in general.[309]

Concerning the GDPR, two issues pointing to the intrinsic constraints of certification systems can be identified, namely, the lack of incentive to the implementation of certification systems and its lack of legal value.[310] The certification procedure is time-consuming and expensive, therefore an incentive should be provided to the controller to invest in the implementation of certification in its processing systems.[311] However, the GDPR is "silent" regarding the promotion of investment incentives. Also, a constraint of certification systems lays in its lack of legal value, confirmed by the GDPR on its article 42 (4). Certification constitutes only a presumption of conformity, therefore, although in a litigation process a certification might mitigate the risk of sanctions, it will not guarantee impunity. Contrarily, the omission of a certification may be an aggravating factor when in litigation. Again, it is considered that article 42 (1) of the GDPR may contradict itself in its terms, concerning the disparity of investment present between large and small companies, developed and under developed industries.[312]

From 25 May 2018, the EDPB[313] will have the possibility to create a European Data Protection Seal, a common certification. However, the constraints of certification systems makes it hard to trust its effectiveness under the GDPR,[314] especially to ensure transparency of algorithm-based decisions that form the basis of political micro-targeting.

[309] Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).
[310] Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).
[311] *ibid.*
[312] *ibid.*
[313] European Data Protection Board.
[314] Olivia Tambou, 'L'introduction De La Certification Dans Le Règlement Général De La Protection Des Données Personnelles: Quelle Valeur Ajoutée? (The Introduction Of The Certification In The EU General Data Protection Regulation: What Added Value?)' [2016] SSRN <https://ssrn.com/abstract=2768093> accessed 19 May 2018.

5.5. The endless challenge of political micro-targeting to the electorate's right to data protection

Currently, as demonstrated in the previous chapters, not only sensitive data on citizens is being massively collected and processed *stricto sensu* but, such data processing is being hidden from the public. It is under these conditions that algorithmic-based decisions are being taken by political parties towards the electorate, giving rise to the contemporary campaigning technique of political micro-targeting.

The effects of political micro-targeting techniques are undeniable and widely felt throughout the world. Illustrated by the Brexit Referendum[315] that resulted in the UK leaving the European Union, political micro-targeting may not have been the only tool that led to such developments, but it was certainly one of its catalysts. Regarding this, it is acknowledged that the purposes for which the data subjects submit their personal data are being subverted, the data subjects share their data to a purpose that is posteriorly being used to justify the processing of data for different purposes. Just because the personal data on the electorate is reachable it does not mean that it is legitimate to take it, in secrecy, to the benefit of third parties. Nevertheless, assuming such data processing is deemed legitimate, the lack of transparency in political micro-targeting becomes one issue of crucial importance due to the damage it may do to the democratic system, our political system, that despite different believes is what we aim to secure. Political micro-targeting may undermine democracy or at least change the way we perceive it. Bearing this in mind, one may question the acceptability of the processing of sensitive data on the electorate.

Democracy and the 'the power of the people' are synonyms. However, power depends on the freedom and knowledge. Freedom for the electorate to choose and decide in what they believe is the best choice, with knowledge of all facts on the options provided, free from coercion and pressure. If freedom and knowledge are constrained, there can be no power of the electorate.[316] The choice of each individual influences society as a whole, therefore, "the common interest is served with everyone's ability to make their choices in complete freedom, and with complete knowledge".[317]

[315] See above paragraph 2.5.3.2.
[316] Sophie Veld, 'On Democracy' (2017) 6 Internet Policy Review.
[317] Sophie Veld, 2017.

It is no great novelty that political communication traditionally uses all kinds of sales tricks and incessantly tends to test the limits of the socially and legally acceptable. However, the way in which you reach the electorate is important to the democratic process, especially concerning the large scale usage of personal data. But where exactly do we stand towards the opacity in data processing promoted by political parties? The freedom and knowledge of the electorate are constantly being jeopardised by political micro-targeting techniques, which manipulate and limits the public discussion. Every time the voter is reached individually with a message tailored to his profile, influenced by targeted personalised messages from a political party or not, not only the voter's access to knowledge is manipulated but, most importantly the public discussion is influenced and limited, always in secrecy. Also concerning, is the misuse of data when data analytics is employed to attack, undermine, discredit or blackmail, constraining critical voices, opposition, and checks and balances.[318] Bearing this in mind, one may ask, if the knowledge available to voters is manipulated to his inner interests and personal needs without them knowing, how can the electorate have knowledge of all facts to make a conscious decision? If the access to knowledge is being deliberately undermined, behind voter's "back", is the electorate really free to choose, is there really a democracy?

The usage of data storage devices and networks is an undeniable reality nowadays. Political parties may continue data processing on the electorate, with or without complying with data protection legislation. And the data protection transparency principle may continue to be infringed, unless effective guarantees to respond to this issue are provided.[319]

Considering the above, the regulation and limitation of the use of personal data, especially sensitive data, is essential to guarantee the elevation of the democratic system in a world that revolves around technological advancements. Safeguards are needed to ensure the freedom of people in their choices and equal and fair access to knowledge in order to promote the public discourse. As such, in a world where the influence of technology on political campaigning substantially changing the relationship between candidates, parties, voters and the media,[320] I stand for a rigorous application of the GDPR but, especially for a rigorous enforcement of the transparency principle. Only when the political party's informational duties, concerning sensitive

[318] Sophie Veld, 2017.
[319] Bert-Jaap Koops, 2010: 326-333.
[320] Colin J. Bennett, 2013.

data processing on the electorate, are complied with, the democratic system can aim to be assured. Therefore, it must be guaranteed that clear and meaningful information with regard to data processing on voters is provided to them before targeting them, before a choice is made. The informational rights must be complied with and secured so the transparency required to data processing is assured.

Hildebrandt seems to be of the opinion that data protection is ineffective in combating the negative aspects of profiling,[321] considering the failure of the legislation to effectively guarantee its core values such as, transparency.[322] Nonetheless, Koops thinks that data protection "can still make a difference (at least to the extent that data protection is effective at all) considering the counter-developments of new tools of transparency becoming available to citizens". However, he also states that "given the caveats of counter-developments and potential shifts in the social context, it is still possible that profiling is a threat to citizens".[323]

Bearing in mind the mechanisms provided by the GDPR to enhance transparency, I have to humbly agree with Koops opinion.[324] Considering the discussed earlier in the previous chapter, the effectiveness of the remedies provided may be questionable considering political parties keep hiding their activity, even though subjected to the transparency of data processing principle. From 25 May 2018, considering the data processing by political parties are subject to the GDPR core principles and rules such as, the transparency obligations established. The continuous noncompliance with such obligations will entail newly burdensome administrative fines,[325] thus the Regulation may provide enough incentive to comply with such obligations. Even so, preventive measures should be simultaneously considered to secure the transparency of data processing of the electorate and their correspondent rights, of which the discussed DPbD, the DPIA's and the certification system are enlightening examples, although ambiguous ones for now.[326] So, I agree data protection may actually make a difference but, it is questionable how significant that change might be.

[321] One of the 'crucial tools' of political micro-targeting. See above paragraph 2.3.1.1.
[322] Mireille Hildebrand, 2010: 303-343.
[323] Bert-Jaap Koops, 2010: 326-333.
[324] Bert-Jaap Koops, 2010: 326-333.
[325] Article 83 of the GDPR and recitals 148 to 152 of the GDPR.
[326] See above paragraphs 5.2. and the following.

Although, the heaviness of the fines established in the GDPR is new, the duty of political parties to inform the data subjects when processing sensitive data on them is not a novelty. So, the referred preventive measures newly established in the Regulation have to be considered jointly with the fines, even though its efficacy remains unclear. This is not only to prevent the electorate's rights of being undermined but also to create the sense of obligation in third parties to comply with the obligations effectively enshrined in the GDPR.

Also, concerning is the rapid technological advancement which political campaigning techniques follow and that the GDPR measures must keep up with to grasp the constant challenge that is the compliance with the transparency principle.

Finally, the ultimate challenge to secure the transparency of data processing on the electorate and the most concerning, in my opinion, will be to answer to the complexity underlying algorithms, since the GDPR does not a provide a specific 'formula' for such issue. The complexity of the algorithm demands more than an empty fulfilment of an obligation of transparency, but requires the electorate comprehension of the mechanisms and consequences underlying the algorithmic-based decisions taken in the 'micro-targeting' process.

Consequently, considering the recent case studies and the difficulties to ensure the transparency principle and comply with its correspondent obligations as enshrined in the data protection framework, the data protection framework is currently failing to assure the electorate's right to data protection, considering its core value of transparency of data processing. Thus, we can only hope the newly enforced mechanisms contemplated in this chapter work efficiently to ensure a transparent data processing prosecutor of democracy.

Transparency depends on effective enforcement of the remedies established in the GDPR and transparency is the precursor of the democratic system. Therefore, considering the threat that political micro-targeting may still represent to citizens even though new tools to foster transparency are available, I hope the enforcement of the GDPR creatively and effectively answers the challenge that such political campaigning techniques represent to our political system and correspondingly to the electorate rights. Therewith, to ensure that technology-based mechanisms such as, political micro-targeting, enhance Democracy, without undermining its fundamental goals, some recommendations to overcome its social and legal limitations are proposed in the last chapter, on "Recommendations".

5.6. Conclusion

According to the GDPR, new mechanisms were introduced that may promote compliance with the transparency principle namely, DPbD, DPIAs and certification systems. Although there are encouraging prospects towards their implementation regarding algorithmic decision-based systems such as, political micro-targeting, the limitations inherent to the solutions as formulated in the GDPR make its effectiveness doubtful until the Regulation is enforced from May 2018.

Considering the inefficacy of data subjects information and access rights towards enhancing transparency and the uncertainty of application of mechanisms that might constitute a solution in the future to the effective enforcement of the transparency principle, it is questioned what consequences the opacity of data processing might entail to the electorate in the EU.

Democracy is defined by the freedom and knowledge that of electorate, which is guaranteed through the transparency of processing in an algorithm dependable world of politics driven by political micro-targeting. Therefore, transparency is crucial to secure the right to data protection of the electorate and subsequently, its position in the democratic system.

However, presently, the transparency principle is not being effectively guaranteed in the 'micro-targeting' scenario. The safeguards provided by the GDPR towards enhancing transparency are inefficient, and the guarantees newly available in the GDPR, that must complement the newly burdensome administrative fines remain a novelty. The heaviness of the fines established in the GDPR is new, but the duty of political parties to inform the data subjects when processing sensitive data on them is not. So, the preventive measures newly established in the Regulation must be considered jointly with the fines, even though its efficacy remains unclear.

Political campaigning and the rapid technological advancement go hand in hand and oblige the GDPR measures to keep up with it consequently, to grasp the constant challenge that is the compliance with the transparency principle. Also, the major challenge that is the complexity underlying algorithms, must be answered since the complexity of the algorithm demands more than an empty fulfilment of an obligation of transparency. It requires the electorate comprehension of the mechanisms and consequences underlying the algorithmic-based decisions taken in the 'micro-targeting' process.

Thus, considering the difficulties to ensure the transparency principle and comply with its correspondent obligations as enshrined in the GDPR, the data protection framework is currently failing to assure the electorate's right to data protection, considering its core value of transparency of processing. Thus, I can only hope the newly enforced mechanisms contemplated in this chapter work efficiently to ensure a transparent data processing prosecutor of democracy.

The enforcement of the transparency principle to guarantee the integrity of democracy will rely deeply on the efficient and creative implementation of the newly implemented measures in the GDPR that must keep up with the fast technological developments on politics.

6. Conclusion

6.1. Answering the research questions

The influence of technology in political campaigning is felt for several years now. However, with the maturing of the Internet and the associated new forms of communicating, through virtual networks, innovative forms of approaching citizens emerged such as, political micro-targeting.

Political micro-targeting represents partially the change from creating a message for mass audiences to tailoring messages to a targeted audience, based on data analytics. Through predictive modelling techniques, political parties divide potential voters into small groups according to their characteristics and then target them accordingly, in an attempt to change their behaviour at the ballot box. This technique is usually based in micro profiling of the behavioural characteristics of the electorate, process enabled by Big Data analytics and enhanced by complex and accurate algorithms. Consequently, political micro-targeting is not harmless and may entail adverse impacts on citizens namely, the risk of *dataveillance.* Apart from being constantly watched, people might be 'watched' without noticing it, raising a concern on transparency of data processing. Such suspicion although evident for some, is confirmed today to the public in the field of politics, according to the 'Cambridge Analytica' case.

Even though the European political culture exhibits a general distrust upon intrusive political campaigning techniques as such, supported by a strict privacy and data protection framework, nowadays, case studies in The Netherlands, Germany and the UK, have shown that data-driven politics is a predominant procedure in European politics. Today, it is proven that political parties are micro-targeting voters in Europe. Profiles are made on the electorate, mainly based on Facebook data, without them knowing their data is being processed for such purposes. The electorate has no clue how political micro-targeting is developed or even if it is being developed. That is why this contemporary political campaigning practice is illustrative of a huge transparency issue.

Additionally, apart from the opacity surrounding political micro-targeting, one of its most concerning risks is the possibility that 'micro-targeting' leads to deceptive, discriminatory or

unethical outcomes with regard to informational content asymmetries. Also, it may be considered an intrusive practice to one's (subject to the decisions) autonomy, if the behaviour and consequently the freedom of choice of the voter is destabilised. Still, without knowledge over the process embed in 'micro-targeting', it is impossible to assess how risky the approach might be, or even if it takes place. Therefore, a necessity to empower the electorate arise, so such consequences are avoided and the concerned parties are held accountable for the deemed infringements to the rights and freedoms of the electorate.

Hence, the empowerment of the electorate can be obtained through transparency, since, it is believed that only the "observation produces insights which create the knowledge required to govern and hold systems accountable". However, transparency is not just "a precise end state in which everything is clear and apparent," but implies knowledge over what is observed. Thus, transparency is obtained as long as the information given to the public is visible, discernible and understandable, making political micro-targeting clear to the concerned parties, then enabled to scrutinize the targeting technique and hold the concerned parties accountable.

Contrarily to what recent practices have shown, transparency is also one of the core values of the European data protection legislation and it must be effectively guaranteed according to the GDPR, not only as an ideal value to aim when processing personal data but as a promise of openness to the electorate, accountability of the parties involved and autonomy of the users, subsequently creating the prospect of making easier to regulate the behaviour of the actors in a democratic society. Therefore, it is important to firstly dismantle what political micro-targeting specifically means to the European data protection regulation, so solutions can be posteriorly found to address the transparency issue surrounding political micro-targeting in a democratic society.

Political parties decide on which individual to target with advertisement, based solely on the results provided by an algorithm that constructs on citizens profiles showing the personalities more susceptible to certain kinds of messages and ideas as well as political preferences or other interests of the voter. The voters access to knowledge is being restricted and manipulated therefore, the electorate voting rights that must be exercised free and consciously are significantly biased where political micro-targeting is based on behavioural profiling. Such effect qualifies political micro-targeting as automated decision-making for data protection purposes. According to the GDPR, political micro-targeting involves solely automated decision-making, including profiling.

GDPR, making the rules of its article 22 applicable in addition to the general provisions applicable to profiling.

As mentioned above, political micro-targeting is a process usually shrouded in secrecy, raising concerns on opacity and unintelligibility as well as on the ruthless outcomes it may take namely, discrimination and manipulation of access to knowledge. Therefore, the obligations that are imposed on the GDPR to controllers must be considered so as to guarantee clarity to data subjects on data processing on them.

According to article 12 (1) GDPR, it is the controller's obligation to guarantee not only a lawful basis for processing but also all the relevant information on the processing of personal data must be provided to the data subject, given the potential risks involved in profiling.

Such risks are only intensified by "ubiquitous-computing developments" such as, the technical and complex algorithms embed in the 'micro-targeting' process. Its characteristics makes them hardly explainable by the specialists or comprehensible by the public leading to the opaqueness of the decision-making. Hence, if the decision is not known or the factors underlying automated decision-making understandable, the assessment of its negative effects becomes impossible. Thus, a need for algorithmic transparency arises not only to prevent effects like discrimination, but also to determine the distribution of accountability in automated decision-making.

Algorithmic transparency strives for "openness about the purpose, structure and underlying actions of the algorithms used to search for, process and deliver information", constituting an important tool towards understanding of the reasons behind biased decision-making which would consequently be primordial towards preventing algorithmic discrimination and, most importantly to unravel the existence of the process itself.

Due to the secrecy embed in political micro-targeting techniques, it becomes obvious that the controller's transparency obligations under the GDPR are not being guaranteed.

The data subjects should be informed of data processing activities concerning themselves to ensure the compliance with the transparency principle under the GDPR but, most of all, to permit

them to effectively exercise their rights in relation to the processing of their personal data, to ensure accountability of the concerned parties.

Hence, the rights established in the Articles 13 to 15 of the GDPR namely, the right to be informed of the data processing and the right to access of the data subject are the foundation of the safeguards to automated decision-making. These rights assure the communication with the data subject, and for that reason are building blocks of the transparency obligations. The way data is processed must be clearly and sufficiently comprehensible so that an individual can exercise his/her rights according to the GDPR. However, presently, it is questionable if these rights are being effectively secured or even contribute to guarantee the transparency of data processing.

Firstly, although information on the existence of data processing may be provided to the data subjects, this right is easily undermined by the parties interested in keeping data processing in secrecy, as it happened to the electorate in the UK. Secondly, even if the information on data processing is conceded, the profiling techniques involved in 'micro-targeting' can be intricate to the average person to understand.

Nonetheless, the right of access, may turn out to be a powerful instrument to provide transparency of data processing to data subjects. However, its success strongly depends on the future interpretation of the indeterminate restrictive, unclear or even paradoxical concepts embodied in the respective provision. Thus, one must ask if the provisions as established in the GDPR satisfy the transparency that should be intrinsic to data processing activities.

At present, it is considered that the GDPR does not guarantee transparent and accountable automated decision-making since the transparency warranties conceded to the data subjects under the GDPR are being firmly challenged. At best, the 'right to be informed' about the existence of automated decision-making and system functionality may be successfully granted if effectively enforced. However, the right of access faces a few obstacles besides its ambiguous core concepts.

First, the lack of awareness or understanding of the public regarding the technicalities of political micro-targeting holds back an effective enforcement of the right. Second, the obstacles are exacerbated if the right to information is not complied with in first place, as is often the case in political campaigning. So, even if there is a possibility that information on the automated decision-making process is disclosed, the electorate has no insight into the actual practice of contemporary campaigning taking place. Lastly, if the choice to provide such information is on

the political parties 'hands' only, it is likely that transparency of processing keeps being undermined due to the campaigning interests of political parties. Therefore, the guarantees are diminished and as the electorate becomes more vulnerable concerning developing technologies, measures urge to be considered.

It is crucial to analyse the GDPR remaining mechanisms that may be able to guarantee the transparency of data processing, especially in the particular case of political micro-targeting, where the electorate position in the democratic system is at stake.

According to the Regulation, new mechanisms were introduced that may promote compliance with the transparency principle namely, DPbD, DPIAs and certification systems. Although there are encouraging prospects towards their implementation, the limitations inherent to the solutions as formulated in the GDPR make its effectiveness doubtful until the Regulation is enforced from May 2018.

Considering the inefficacy of data subjects information and access rights and the uncertainty of application of mechanisms that might constitute a solution in the future to the effective enforcement of the transparency principle, the consequences of the opacity of data processing to the electorate in the EU must be weighted.

Freedom and knowledge, the corollaries of democracy, can only be guaranteed through the transparency of processing. Therefore, as regards to political micro-targeting, transparency is crucial to secure the fundamental right to data protection of the electorate and its position in the democratic system.

However, the transparency principle is not being guaranteed. The safeguards provided by the GDPR towards enhancing transparency are inefficient, and the guarantees newly available remain a novelty and its efficacy remains unclear.

Political campaigning techniques and the rapid technological advancement go hand in hand and oblige the GDPR measures to keep up with it consequently, to grasp the constant challenge that is the compliance with the transparency principle. Moreover, the complexity underlying algorithms remain one of the major transparency challenges. The complexity of the algorithm demands more than an empty fulfilment of an obligation of transparency. It requires the electorate

comprehension of the mechanisms and consequences underlying the algorithmic-based decisions taken in the 'micro-targeting' process.

Thus, considering the difficulties to ensure the transparency principle as enshrined in the GDPR, right now the data protection framework is failing to assure the electorate's personal data protection, as regards to its core value of transparency of processing.

Accordingly, the enforcement of the transparency principle, basis of the integrity of democracy will rely deeply on the implementation of the newly measures established under the GDPR. Therefore, a few recommendations on how to effectively ensure transparency while limiting the power provided to the political parties will follow.

6.2. Recommendations

While it is advised that the concerned parties start revising their current consent forms, privacy statements, customer information notices, etc.[327], measures must be proposed to tackle the transparency issue on an earlier stage.

To foster transparency of profiling techniques, considering its characteristic risks[328], Koops[329] suggests a specific measure to be built into technology, the profile 'flags'. These would be developed to appear when a profile-based decision was taken[330], to inform data subjects profiling techniques are occurring using their personal data. The data subject would be informed in an early stage and their rights could be exercised, like the right to contest the profiling-based decision.

[327] Voigt, P., Bussche, & A. (2017). *The EU general data protection regulation (GDPR): A practical guide*. Cham: Springer International Publishin. P.147.
[328] See above paragraph 2.4.
[329] Bert-Jaap Koops, 'Some Reflections On Profiling, Power Shifts And Protection Paradigms'', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010): 336.
[330] Regarding this possibility an enlightening example is given: "In on-line service delivery, for example, when someone is denied a request, the web page could automatically show a 'profile icon', perhaps linking to information about the profile used. In offers, a flag should show up indicating that the offer has been made on the basis of a profile – comparable to on-line shops showing advertisements such as: 'People who bought The Da Vinci Code also bought The New Testament'. Moreover, if profile use leads to not making an offer, this should likewise be mentioned somewhere by showing a profile icon. Ideally, a tool should be available for people to click on a link showing the precise personal data that were used as input in the profile, so that they know that the offer – or non-offer, or the decision upon a request – was based on their clickstream, search words, IP-addressinferred country of origin, credit history and/or use of a Microsoft browser, to name a few possible criteria." In Bert-Jaap Koops, 2010: 336.

Also, the Article 29 WP recommends with regard to profiling, "specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles" as well as the use of anonymization or pseudonymization techniques to safeguard the electorate right to data protection.

In the field of political micro-targeting where massive amounts of data are gathered daily to be built into profiles of voters, I strongly believe that the incorporation of such measures into technology would ease the implementation and the compliance with the data protection principles while enhancing the protection of the electorates' data from an early stage on, preventing it from further abuse. However, in line with Koops thoughts[331], I do not think the implementation of such measures into technology should weigh on the industry since, as stated in chapter 2[332], political micro-targeting techniques secrecy is fomented by the industry itself. In the case of political micro-targeting, political parties show no interest in displaying such techniques to the public for the benefit of the political campaigning. Thus, the development of "transparency by design" should be stressed not only by civil society, whose rights are at stake, but mostly by the data protection authorities, so, appropriate enforcement of the transparency principle required under the GDPR is ensured, bearing in mind the specificity of the current situation.

Within this framework of thought, control mechanisms should be established, to ensure adequate enforcement of the law since "individual complaints have little power in a ubiquitous profiling world"[333], when they are possible. So, Koops[334] proposes that a Profiling Authority is established to monitor profiling practices, not only to handle complaints but also to actively investigate such practices.

Hence, to make the best out of the proposed solutions, it is crucial to promote education in algorithm literacy of the data subjects to respond to the 'algorithm-ization'[335] of political campaigning while enforcing accountability.

Finally, with regard to the 'Cambridge Analytica' scandal in specific, preventive measures are currently being thought and allegedly enforced to promote transparency of data processing in such

[331] Bert-Jaap Koops, 2010: 337.
[332] See above paragraph 2.6.
[333] Bert-Jaap Koops, 2010: 337.
[334] Bert-Jaap Koops, 2010: 337.
[335] Lee Rainie and Janna Anderson, 'Code-Dependent: Pros And Cons Of The Algorithm Age' [2017] Pew Research Center <http://www.pewresearch.org> accessed 27 May 2018.

peculiar situations. According to Mark Zuckerberg, in declarations to the European Parliament[336], not only audits on Facebook apps are being conducted, but also measures to limit the access to information on data subjects and to ensure its legitimacy and clarity are being taken. Also, pursuing the claim of "making advertisement on Facebook much more transparent", a new tool, "View Adds"[337], was created. Considering this, I am personally sceptical but thrilled for further developments and hopeful to see not only the data subjects reaction but also how the political parties, the controllers, and intermediaries' will cope with the increasing importance of transparency in political campaigning.

6.3. Limitations

As regards to the limitations of this thesis, it is essential to delineate the theme's scope, temporally and materially.

First, to refer that this research was conducted from October 2017 to May 2018. Only in March 2018 details on the UK 'Cambridge Analytica' case were published, which brought to light the reality of political micro-targeting and correspondent concerns to the public. Now that the functioning of 'micro-targeting' and the responsible entities are out, it is expected that plenty of research will be conducted in a near future. Therefore, I sincerely hope the development of the transparency principle regarding political micro-targeting, one of the core values of data protection, serves as food for thought not only for the academia but, for the actors involved with the power to change the reality we live in, to one more protective of our personal data and our freedom in a democratic society.

Second, even though the theme of this thesis is closely related to other core principles of data protection such as, the purpose limitation or data minimisation, highly conflicting with political

[336] European Parliament, 'LIVE: Parliament'S Leaders Are Discussing With Facebook CEO Mark Zuckerberg About Data Privacy' (European Parliament Facebook Page 2018).
[337] This tool "let you see all of the adds that any page is running. So, now you can see all the different messages that an advertiser or a political actor, are sending to all of the different audiences they are trying to reach". In European parliament, 2018.

micro-targeting, these are not being developed on this thesis whose main focus is the transparency of data processing carried out for political micro-targeting purposes.

Lastly, it is assumed that political micro-targeting is a practice deemed legitimate for research purposes. However, I hope the discussion on the legal and legitimate grounds the processing of sensitive data for political campaign purposes is developed, since important European elections are happening soon and, in my opinion, it is important to define the conditions in which contemporary campaigning practices may occur, so the electorate is properly protected.

Bibliography

Monographs

Hildebrandt MS Gutwirth, *Profiling The European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Kreiss D, 'Digital Campaigning', *Handbook of Digital Politics* (Edward Elgar 2018).

Kreiss D, 'Prototype Politics: Technology-Intensive Campaigning And The Data Of Democracy' *Oxford University Press* (2016).

Nielsen R, *Ground Wars* (Princeton University Press 2012).

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money And Information* (Harvard University Press 2015).

Solove D, *The Digital Person. Technology And Privacy In The Information Age* (New York University Press 2004).

Voigt PA Bussche, 'The EU General Data Protection Regulation (GDPR): A Practical Guide' [2017] Springer International Publishing.

Articles and Papers

Abramson A, 'Cambridge Analytica Whistleblower Tells U.K. Lawmakers His Predecessor Was Poisoned' [2018] *TIME* <http://time.com/5216680/cambridge-analytica-christopher-wylie-predecessor-poisoned/> accessed 10 April 2018.

Ananny MK Crawford, 'Seeing Without Knowing: Limitations Of The Transparency Ideal And Its Application To Algorithmic Accountability' (2016) 20 New Media & Society.

Anstead N, 'Data-Driven Campaigning In The 2015 United Kingdom General Election' (2017) 22 The International Journal of Press/Politics.

Bayamlloolu E, 'Transparency Of Automated Decisions In The GDPR: An Attempt For Systemisation' [2018] SSRN Electronic Journal.

Bennett C, 'How Campaign 'Micro-Targeting' Works? And Why It Probably Doesn't.' *iPolitics* (2015) <http://ipolitics.ca/2015/09/09/how-campaign-micro-targeting-works-and-why-it-probably-doesnt> accessed 18 May 2018.

Bennett C, 'The Politics Of Privacy And The Privacy Of Politics: Parties, Elections And Voter Surveillance In Western Democracies' [2013] SSRN Electronic Journal.

Bennett C, 'Voter Databases, Micro-Targeting, And Data Protection Law: Can Political Parties Campaign In Europe As They Do In North America?' (2016) 6 International Data Privacy Law.

Bennett C, 'Voter Surveillance, Micro-Targeting And Democratic Politics: Knowing How People Vote Before They Do' [2014] SSRN Electronic Journal.

Borgesius and others, 'Online Political Microtargeting: Promises And Threats For Democracy' (2018) 14 Utrecht Law Review.

Brkan M, 'Do Algorithms Rule The World? Algorithmic Decision-Making In The Framework Of The GDPR And Beyond' [2017] SSRN Electronic Journal.

Cadwalladr C, ''I Made Steve Bannon'S Psychological Warfare Tool': Meet The Data War Whistleblower' *The Guardian* (2018).

Cadwalladr CE Graham-Harrison, 'How Cambridge Analytica Turned Facebook 'Likes' Into A Lucrative Political Tool' *The Guardian* (2018) <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> accessed 5 April 2018.

Cadwalladr CE Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested For Cambridge Analytica In Major Data Breach' *The Guardian* (2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 5 April 2018.

Centre for Information Policy Leadership Hunton & Williams LLP, 'Certifications, Seals And Marks Under The GDPR And Their Role As Accountability Tools And Cross-Border Data Transfer Mechanisms' (Centre for Information Policy Leadership GDPR Implementation Project 2017).

De Hert PH Lammerant, *Predictive Profiling And Its Legal Limits: Effectiveness Gone Forever* (Amsterdam University Press/WRR 2016).

Dobber T and others, 'Two Crates Of Beer And 40 Pizzas: The Adoption Of Innovative Political Behavioural Targeting Techniques' (2017) 6 Internet Policy Review <http://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-politicalbehavioural-targeting> accessed 7 January 2018.

Doward JA Gibbs, 'Did Cambridge Analytica Influence The Brexit Vote And The US Election?' *The Guardian* (2017).

Edwards LM Veale, 'Enslaving The Algorithm: From A Right To An Explanationn To A Right To Better Decisions?' [2017] SSRN Electronic Journal.

Edwards LM Veale, 'Slave To The Algorithm? Why A Right To Explanationn Is Probably Not The Remedy You Are Looking For' [2017] SSRN Electronic Journal.

Glaser A, 'Potential Lawsuit Could Reveal How Trump Targeted Voters On Facebook And If There'S Any Connection To Russia' <http://www.slate.com/blogs/future_tense/2017/10/06/possible_british_lawsuit_could_reveal_how_cambridge_analytica_targeted_voters.html> .

Gonzalez Fuster G, 'The Emergence Of Personal Data Protection As A Fundamental Right Of The EU, Springer International Publishing, 2014, 274 Pp, ISBN 978-3-319-05022-5' (2017) 5 International Data Privacy Law.

Gorton W, 'Manipulating Citizens: How Political Campaigns' Use Of Behavioral Social Science Harms Democracy' (2016) 38 New Political Science.

Gutwirth SP De Hert, 'Regulating Profiling In A Democratic Constitutional State', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Hildebrandt M, 'Defining Profiling: A New Type Of Knowledge?', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Hildebrandt M, 'Profiling And The Identity Of The European Citizen', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Information Commissioner's Office (ICO), 'Big Data, Artificial Intelligence, Machine Learning And Data Protection'.

Kokott JC Sobotta, 'The Distinction Between Privacy And Data Protection In The Jurisprudence Of The CJEU And The Ecthr' (2013) 3 International Data Privacy Law.

Koops B, 'Some Reflections On Profiling, Power Shifts And Protection Paradigms'', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Koops BR Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology.

Kreiss D, 'Yes We Can (Profile You): A Brief Primer On Campaigns And Political Data' [2012] *Stanford Law Review Online* https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/.

Kruschinski SA Haller, 'Restrictions On Data-Driven Political Micro-Targeting In Germany' (2018) 6 Internet Policy Review.

Lachaud E, 'Quelle Peut Tre La Contribution De La Certification La Protection Des Donnnes Personnelles? (What Can Be The Contribution Of Certification To The Data Protection?)' [2017] SSRN Electronic Journal.

Marcus R, 'Germany'S Throwback Campaign' *The Washington Post* (2013) <https://www.washingtonpost.com/opinions/ruth-marcus-germanys-throwback campaign/2013/09/24/14043b4e-2540-11e3-ad0d b7c8d2a594b9_story.html?noredirect=on&utm_term=.85aa8883ca2c> accessed 18 May 2018.

Mendoza IL Bygrave, 'The Right Not To Be Subject To Automated Decisions Based On Profiling' [2017] EU Internet Law.

Norris P, 'The Evolution Of Election Campaigns: Eroding Political Engagement?' [2004] Paper for the conference on Political Communications in the 21st Century.

Pawelczyk P, J JakubowskiP Politologiczny, 'Political Marketing In The Times Of Big Data'.

Rainie LJ Anderson, 'Code-Dependent: Pros And Cons Of The Algorithm Age' [2017] Pew Research Center <http://www.pewresearch.org> accessed 27 May 2018

Rubinstein I, 'Big Data: The End Of Privacy Or A New Beginning?' (2013) 3 International Data Privacy Law.

Rubinstein I, 'Voter Privacy In The Age Of Big Data' [2014] SSRN Electronic Journal.

Scherer M, 'Friended: How The Obama Campaign Connected With Young Voters' [2012] *Time.*

Tambou O, 'L'introduction De La Certification Dans Le Règlement Général De La Protection Des Données Personnelles: Quelle Valeur Ajoutée? (The Introduction Of The Certification In The EU General Data Protection Regulation: What Added Value?)' [2016] SSRN <https://ssrn.com/abstract=2768093> accessed 19 May 2018.

The Economist, 'Campaigning In Germany' (2017) <https://www.economist.com/news/europe/21728994-new-technology-has-brought-door-door-campaigning-continental-europe-campaigning-germany> accessed 18 May 2018.

The End Of Privacy, Keynote At Cebit'17 (2017).

Timberg CK Adam, 'Christopher Wylie: How Cambridge Analytica's Whistleblower Became Facebook's Unlikely Enemy' *Independent* (2018) <https://www.independent.co.uk/news/long_reads/christopher-wylie-cambridge-analytica-facebook-data-breach-whistleblower-trump-election-a8267991.html> accessed 10 April 2018

Trent J, R FriedenbergR Denton, *Political Campaign Communication* (Rowman & Littlefield 2011).

Turow J, *The Daily You: How The New Advertising Industry Is Defining Your Identity And Your Worth* (2011).

Van der Hof SC Prins, 'Personalisation And Its Influence On Identities, Behaviour And Social Values', *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2010).

Veld S, 'On Democracy' (2017) 6 Internet Policy Review.

Wachter S, B MittelstadtL Floridi, 'Why A Right To Explanation Of Automated Decision-Making Does Not Exist In The General Data Protection Regulation' (2017) 7 International Data Privacy Law.

Zuiderveen Borgesius F, 'Improving Privacy Protection In The Area Of Behavioural Targeting' [2015] SSRN Electronic Journal.

European Union Sources

Article 29 Data Protection Working Party, 'Guidelines On Automated Individual Decision-Making And Profiling For The Purposes Of Regulation 2016/679 (17/EN WP 251)' (European Commission 2017).

Chair of the Article 29 Working Party, 'Cambridge Analytica – Reaction' (2018).

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION [2000] OJ 1 364/1.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31.

European Parliament, 'LIVE: Parliament’S Leaders Are Discussing With Facebook CEO Mark Zuckerberg About Data Privacy' (European Parliament Facebook Page 2018).

'Explanatory Text For Proposal For A Council Directive Concerning The Protection Of Individuals In Relation To The Processing Of Personal Data, COM (90) 314 Final – SYN 281'.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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) [20017] OJ 2 119/1.

Other Sources

(www.dw.com) D, 'CDU, SPD And Greens Use Big Data To Target Bundestag Voters | DW | 26.08.2017' (*DW.COM*, 2018) <http://www.dw.com/en/cdu-spd-and-greens-use-big-data-to-target-bundestag-voters/a-40244410> accessed 23 May 2018.

Channel 4 News, 'Revealed: Trump'S Election Consultants Filmed Saying They Use Bribes And Sex Workers To Entrap Politicians' <https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation> accessed 18 May 2018.

Concordia, 'Cambridge Analytica - The Power Of Big Data And Psychographics' <https://www.youtube.com/watch?v=n8Dd5aVXLCc> accessed 7 February 2018.

Electronic Privacy Information Center, 'EPIC - EPIC Promotes 'Algorithmic Transparency' For Political Ads' (2017) https://epic.org/2017/11/epic-promotes-algorithmic-tran-1.html.

Goodman E and others, 'The New Political Campaigning' (The London School of Economics and Political Science 2017).

'Social Media: Censorship Against Freedom Of Speech' https://medium.com/@khalilkafa/social-media-censorship-against-freedom-of-speech-76603634c2d9.

Song C and others, 'Limits Of Predictability In Human Mobility' (2010) 327 Science.

The Guardian, 'Cambridge Analytica Whistleblower: 'We Spent $1M Harvesting Millions Of Facebook Profiles' <https://www.youtube.com/watch?time_continue=4&v=FXdYSQ6nu-M> accessed 23 May 2018.

The Guardian, 'The Brexit Whistleblower: 'Not Cheating Is The Core Of What It Means To Be British' https://www.youtube.com/watch?v=7vo1u9JRZG8&index=4&list=PLa_1MA_DEorHSyKo2uelblYGZLP6e4Cyg.

The Guardian, 'What Is The Cambridge Analytica Scandal?' <https://www.youtube.com/watch?v=Q91nvbJSmS4> accessed 25 March 2018.

Upturn, 'Data Brokers In An Open Society' (Open Society Foundations 2016).

'What Is Algorithmic Transparency? - Definition From Whatis.Com' (*SearchEnterpriseAI*, 2018) https://searchenterpriseai.techtarget.com/definition/algorithmic-transparency.