Master's Thesis:

Political Profiling: from the US to the EU, data protection regulation from a transatlantic perspective

Aikaterini Pouliou

LL.M. Law and Technology

2017-2018

Title: Political Profiling: From the US to the EU, data protection regulation from a transatlantic perspective.

Master's Thesis by Aikaterini Pouliou

SNR: 2008650

Tilburg University

Tilburg Institute of Law, Technology and Society (TILT)

Master's Program in Law and Technology (LL.M.)

Thesis defense: January 2018

Thesis supervised by Drs. Bart van der Sloot and PhD Researcher Irene Kamara.

List of abbreviations

Art.29WP	Article 29 Working Party
DPA(s)	Data Protection Authority(-ies)
DPD	Data Protection Directive
EDPS	European Data Protection Supervisor
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
PAC	Political Ad Collector
PII	Personally Identifiable Information
UK	United Kingdom
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
US	United States

Contents

Introduction

Background

The news that Trump won the elections with the help of big data analytics made headlines earlier this year and there is ever since an ongoing debate concerning the latest revelations on the matter. The elections management agency Cambridge Analytica, which is the one linked to Trump's political campaign and ultimately to the elections outcome,[1] claims to have collected "*up to 5.000 data points per person on over 230 million Americans, using more than 100 data variables to model target audience groups and predict the behaviour of like-minded people*".[2]

Big data analytics is a term that refers to the process of analysing big amounts of collected data in order to gain insight into, inter alia, behavioural patterns and other useful information that enable data analysts to draw conclusions about data subjects and later make decisions based on these findings.[3] A method commonly used when analysing data in such cases is this of "profiling".[4]

Overall, profiling in big data analytics can be used by companies in order to better understand their customers and predict their behaviours. With the use of sophisticated technologies, such as advanced computer algorithms, text mining and social media analytics,[5] they aim to improve their products and/ or services, ultimately enhancing their

[1] In their website, Cambridge Analytica advertise their services and the efficiency thereof, by admitting that they "provided the Donald J. Trump for President campaign with the expertise and insights that helped win the White House, causing the most remarkable victory in modern U.S. political history". They explain what methods they used in order to achieve the end result and emphasise once again that it was their company that lead to the "extraordinary victory of Donald Trump". The website of the company was updated mid-2017. Ca-political.com. (2017). *Donald J. Trump for President*. [online] Available at: https://ca-political.com/index.php/casestudies/casestudydonaldjtrumpforpresident2016 [Accessed 17 Dec. 2017].

[2] Ca-political.com. (2017). *CA Advantage | CA Political*. [online] Available at: https://ca-political.com/ca-advantage [Accessed 17 Dec. 2017].

[3] Gandomi, A. and Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, [online] 35(2), pp.137-144. Available at: http://www.sciencedirect.com/science/article/pii/S0268401214001066?via%3Dihub [Accessed 17 Dec. 2017].

[4] van der Sloot, B. and van Schendel, S. (2016). Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study. *JIPITEC*, [online] 7(3), 110 para 1. Available at: http://www.jipitec.eu/issues/jipitec-7-2-2016/4438 [Accessed 17 Dec. 2017].

[5] Gandomi, supra note 3 at pp.140, 142.

performance.[6] The use of such technologies for profiling purposes is not new in the industries of marketing and advertising. However, their application in other areas, in which there has been relatively limited publicity until recently[7] and where users' data does not reveal a product preference, but a political one, creates concerns for, among others, the privacy and data protection-related rights of the individuals. There is indeed a growing number of companies that collect and use citizens' data for political purposes with some of them even explicitly advertising themselves for "deeply profiling voters".[8] A number of these companies have been linked to major political events around the world, like the aforementioned Trump's election or the Brexit in the UK.[9]

The issue of profiling citizens' online behaviour for political campaigns seems to be more topical than ever to address, since the impact it can have on society as a whole is monumental. Organisations like Privacy International [10] and UK's Information Commissioner's Office (ICO) have acknowledged the matter, expressing their concern over the possible implications these profiling practices for political campaigns might have, inter alia, on citizens' privacy. ICO even announced in May that they are launching a "formal investigation into the use of data analytics for political purposes".[11] In their latest update on the investigation, which at the time of the writing of this thesis it is still ongoing, ICO

[6] Gandomi, supra note 3 at pp. 138, 141.

[7] Bennett, C. (2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, [online] 6(4), p.261. Available at: https://academic.oup.com/idpl/article/6/4/261/2567747 [Accessed 17 Dec. 2017].

[8] Research Now. (2017). *Research Now: U.S. Voter and Political Market Research*. [online] Available at: https://www.researchnow.com/products-services/global-audiences-and-panel/political-panel/?lang=gb [Accessed 17 Dec. 2017].

[9] The Canadian data analytics company AggregateIQ has been in the center of the investigation into data analytics for political purposes, launched by ICO in 2017, as it is believed to have played a pivotal role in the EU Referendum campaign's outcome. ICO confirms that in their latest blogpost regarding the investigation; Denham, E. (2017). Update on ICO investigation into data analytics for political purposes. [Blog] *Information Commissioner's Office blog*. Available at: https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/#more-3192 [Accessed 17 Dec. 2017]. AggregateIQ advertises their involvement with the EU Referendum campaign by quoting the campaign director of the Vote Leave campaign, Dominic Cummings, on their site: "Without a doubt, the Vote Leave campaign owes a great deal of its success to the work of AggregateIQ. We couldn't have done it without them."; Aggregateiq.com. (2017). [online] Available at: https://aggregateiq.com/ [Accessed 17 Dec. 2017]. See also press related to the topic: Freeze, C. (2017). *B.C., Britain investigate role of Canadian tech firm AggregateIQ in Brexit vote*. [online] The Globe and Mail. Available at: https://www.theglobeandmail.com/news/national/bc-britain-investigate-role-of-canadian-tech-firm-aggregateiq-in-brexit-vote/article37340241/ [Accessed 17 Dec. 2017]. **S**ee also supra note 1.

[10] Falchetta, T. (2017). *Hiding in plain sight — political profiling of voters*. [online] Privacy International. Available at: https://privacyinternational.org/node/1460 [Accessed 17 Dec. 2017].

[11] Denham, E. (2017). The Information Commissioner opens a formal investigation into the use of data analytics for political purposes. [Blog] *Information Commissioner's Office blog*. Available at: https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/ [Accessed 17 Dec. 2017].

admitted that the investigation has been proven to be a rather complicated undertaking.[12] The transnational nature of data is what makes such practices worth further investigating into, as companies operating internationally could deploy them in European grounds with great impact on European citizens' privacy-related rights. ICO's announcement for investigation hints that for the time being it remains unclear whether this is currently just a concern for the future or an unexposed reality.[13]

Profiling practices have been claimed to be, among others, opaque and highly intrusive. They have been criticised for their capacity to affect voters' behaviour to the point of manipulation, due to their increased degree of persuasiveness. Profiling practices have the potential to create a chilling effect on individuals in relation to their voting behaviour. Lastly, they could potentially exclude individuals form receiving political communication, hinder public debate and consequently impede their participation to political life, which constitutes a menace to the democratic system. All the aforementioned threats that are linked to political profiling practices are subsequently investigated in this thesis.

Problem statement and research question

With the contingency of US-based[14] companies processing data and engaging in the profiling of European citizens for political reasons, it is interesting to examine whether such practices are regulated, and to what extent, in the two regions, as well as explore the discussions around their regulation or lack thereof, and the points of critique on the matter. The main research question therefore is the following:

---

[12] Denham, E. (2017). Update on ICO investigation into data analytics for political purposes. [Blog] *Information Commissioner's Office blog*. Available at: https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/#more-3192 [Accessed 17 Dec. 2017].

[13] Noteworthy is the fact that Cambridge Analytica claims to have supported over 100 data-driven political campaigns across five continents and has conducted research for a resurgent political party in Italy; Ca-political.com. (2017). *Homepage | CA Political*. [online] Available at: https://ca-political.com/?__hstc=163013475.2ff0ecbfb275b42a8f91421bb1414c04.1506503660662.1506503660662.1506503660662.1&__hssc=163013475.5.1506503660662&__hsfp=2561377333 [Accessed 17 Dec. 2017]. See also supra note 9.

[14] The fact that these companies are US-based does not affect the protection awarded to data subjects in the EU by the upcoming GDPR, since Art. 3 GDPR states that companies that collect personal data or behavioral information from an individual in the EU are subject to the requirements of the GDPR. Reference to the "US-based" element of these companies is made here because profiling practices for political communication purposes are more extensive, for the moment, in the US than they are in the EU. See also Goodman, B. and Flaxman, S. (2016). *European Union regulations on algorithmic decision-making and a "right to explanation"*. 3rd ed. [pdf] New York: University of Oxford, p.2. Available at: https://arxiv.org/pdf/1606.08813.pdf [Accessed 18 Dec. 2017].

How is the profiling of (potential) voters for political communication purposes currently regulated in the US and in the EU, from a data protection perspective, and how could future regulation affect such profiling?

In order for my research to yield concrete results and for the main question to be answered, the following sub-questions are formulated:

1. Which are the legal frameworks regulating the processing of personal data used for political communication purposes in the US and in the EU?

The first chapter introduces the concept of voter data, followed by a brief description of the practices deployed by major political parties in the US for the exploitation thereof. Subsequently the chapter provides a brief outline of the governance of such data, the limitations of the law and the discussions around these limitations, which is deemed necessary in order to gain an understanding of the regulatory differences between the US and the EU, as well as to highlight the contrast between them. In the same chapter a brief overview of the currently applicable European legal framework regarding data used for political purposes is presented; particular emphasis is given on the transition from the DPD to the GDPR and the discussions on the topic of "profiling" as well as the rationale behind its regulation. The first chapter prepares the grounds for the second one, where the European regulatory framework for profiling is thoroughly analysed.

2. How is profiling for political communication purposes regulated under the GDPR?

The second chapter of this thesis is exclusively focused on the regulatory framework as is shaped by the soon to be applicable GDPR. Reference to the DPD is only made where it is imperative for the purposes of better understanding the impending legislation. The first part of this chapter intends to explore the concept of profiling, provide its legal definition under the GDPR and investigate whether political profiling falls within the scope of the Regulation. It then proceeds to examine whether individuals who are subject to political profiling are granted the right to object and the right not to be subject to automated decision-making by the GDPR. It finally examines the provisions related to the processing of special categories of data and their interrelation to political profiling. Gaps or inaccuracies in legislation are pointed out, assessed and critically reflected upon. By the end of this chapter the possible impacts of political profiling on individuals' rights and freedoms become apparent and the rights with which people can react to political profiling are assessed.

3. Are the current regulatory measures enough?

The third and last chapter of this thesis constitutes an attempt to evaluate whether the currently (or the soon to be) applicable regulatory frameworks provide enough safeguards for the individuals who are subject to political profiling. The first part of this chapter revolves around the question whether political profiling should be prohibited in its entirety. Discussions and legal scholars' opinions on the matter are touched upon, and consequently the effectiveness as well as the feasibility of such a prohibition are evaluated. The role of research at this point in time is also weighed upon. The reinforcement of the principle of transparency as an alternative to the prohibition is evaluated. From this perspective, a set of technological developments aiming at enhancing transparency related to political profiling are presented and the role they could potentially play towards shaping future regulation is assessed. By the end of this chapter I will have collected all the necessary information in order to efficiently answer my main research question in the Conclusion of this thesis.

The outcome of the research would not only provide the designation of the stricter legal regime, but would also help identify whether this guarantees safeguards and provides an adequate level of protection for the citizens' privacy and data protection-related rights, both in the US and in the EU.

Significance of the research

The primary objective of this thesis is to provide an elaborate analysis of the framework that regulates the profiling of voters' behaviour with particular focus on the EU regulation, criticize it and discuss the points in the regulatory approach that could be improved in the future. The seemingly ever-expanding phenomenon of the profiling of voters for political communication purposes and its implications have been discussed to a certain extent by communication scholars and political scientists, who have pointed out a number of effects that such practices can have on individuals, as well as on democratic societies. A small number of legal scholars have also published some papers regarding the profiling of voters' online behaviour and its interrelation with their right to privacy; however, research on the topic remains under-developed to date.[15] Additionally, legal scholars seem to lag behind when it comes to their research on the regulation of the profiling thereof, particularly under the upcoming GDPR. Thus, this thesis not only constitutes an attempt to extend the

[15] Bennett, supra note 6 at p.261.

analysis on the matter from the US context to this of the EU, but it also goes one step further from the traditional approach towards the profiling of voters and addresses the subject in a different context, this of its regulation under the GDPR. In doing so, I hope that this thesis could offer the initial basis for further discussions on the regulation, and the extent thereof, of voters' profiling for political communication purposes, which is an issue of legal interest with both social and political extensions.

Limitations of the research

Despite claims that there are benefits from the profiling practices deployed by political parties and big data analytics companies in the course of electoral activities, among which the circulation and communication of political ideas and the realisation of the citizens' right to be adequately informed about candidates' activities in order to make informed choices, which is facilitated by targeted behavioural advertising,[16] the specific focus of this thesis does not allow for further elaboration on the matter. Additionally, due to the limited extent and topic of the thesis, as well as due to the limits posed by my educational background, the ethical and social aspects of the aforesaid profiling practices will not be explored here. Issues such as the effect those practices have or might have on democracy or equal competition opportunities among electoral parties and anything related to the field of social sciences research will not be touched upon. A brief mention of the concerns associated with these practices however is necessary in order to highlight the social relevance of the topic and the importance of its exploration from a legal perspective. It is undeniable though that the impact that political profiling can have on society is significant and that the debate around it will only keep on growing with each new election cycle.

Lastly, due to the contemporary nature of the issue explored in this thesis, there is no relevant case-law to date.[17]

[16] On Cambridge Analytica's website the word "targeted" is used repeatedly, when explaining how they send "targeted messages" and "targeted adverts" to voters and emphasise how "intelligent targeting and sophisticated messaging techniques" can be used in political campaigns. They suggest that such practices can also be effective when applied to the commercial sector. Ca-political.com. (2017). *Donald J. Trump for President*. [online] Available at: https://ca-political.com/index.php/casestudies/casestudydonaldjtrumpforpresident2016 [Accessed 17 Dec. 2017].

[17] Mendoza, I. and Bygrave, L. (2017). The Right Not to Be Subject to Automated Decisions Based on Profiling. In: T. Synodinou, P. Jougleux, C. Markou and T. Prastitou, ed., *EU Internet Law: Regulation and Enforcement*. [online] Springer, Forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855 [Accessed 18 Dec. 2017].

Research and Methodology

For this thesis the doctrinal type of legal research was adopted, which is based to a great extent on the desk research technique that looked into profiling of voters for political communication purposes, legislation and regulation both in the US and in Europe on a federal and EU level respectively.

The model of legal research that is used for this thesis is both the analysis of the "black-letter" of law and the comparative analysis. In order to better approach my main research question and because of the nature of the problem statement, namely the contingency of the US profiling practices for political communication purposes being deployed in European grounds, the comparative analysis approach is deemed necessary. The aforementioned US practices, which constitute the frame of reference, the inspiration for the writing of this thesis, provided the appropriate stimulation to examine the respective practices in the European grounds under the EU legal framework. Profiling of voters is a far more extended and debated issue in the US than in EU, and consequently academic research on the matter is respectively advanced there, which makes the inclusion of the US perspective in the analysis almost indispensable for the purpose of this thesis. The dissimilarity of the legal and political systems in the two continents does not allow an explicit comparison between two specific legal rules, but mainly restricts it to the description and analysis of the two legal systems and their relation with the issue of profiling for political communication purposes. In the second chapter, which is entirely devoted to the study of the provisions of the GDPR related to profiling, the research is purely analytical; the rule of law is described and critically evaluated. Inbuilt gaps and ambiguities of the legislation are pointed out and assessed. Emphasis is given on the law.[18] The desk research was focused on two issues in particular. The first is this of profiling, political profiling and its definition and the second is the regulation thereof and legislation that governs the issue on a US and EU level.

Publications and legislation used in the research were selected by using terms related to the main research question, such as "profiling", "micro-targeting", "political profiling", "profiling voters in the US", "profiling under the GDPR", etc. both in general search engines as well as in OCLC WorldCat union catalogue. The primary sources that were taken into

[18] The terms of doctrinal legal research, black-letter analysis and comparative analysis are used as defined in the Legal Research Methods; Vibhute, K. and Aynalem, F. (2009). *Legal Research Methods*. [ebook] Chilot Wordpress. Available at: https://chilot.files.wordpress.com/2011/06/legal-research-methods.pdf [Accessed 18 Dec. 2017].

consideration include, but are not limited to, the Data Protection Directive (Dir. 95/46EC), hereinafter Directive and the General Data Protection Regulation (Regulation (EU) 2016/679), hereinafter GDPR or Regulation. Complementary legal documents such as Opinions and commentary of the Article 29 Working Party (Art.29WP) and European Data Protection Supervisor (EDPS), as well as opinions and relevant documents of independent privacy and information rights authorities were consulted. Legal scholar books, articles gleaned from legal journals and websites, and legal research papers were also reviewed. Journalistic articles were used where deemed appropriate in relation to the topicality of the issue explored in this thesis. All the sources that were consulted are listed in this thesis.

Benchmarks of the research conducted for this thesis are considered the following; the "Profiling the European Citizen- Cross-disciplinary Perspectives" (M. Hildebrandt and S. Gutwirh, 2008)[19] book was the starting point for the writing of this thesis. It recognises the potential that profiling technologies have in an era when the proliferation of data is unprecedented and constitutes an attempt to define profiling and its effect on the "rule of law and democracy" through a multi-disciplinary approach. This publication has been of paramount importance for my initial research on the topic, since it facilitated the familiarisation with the concept of profiling, provided its definition in light of the absence of a legal one, at the time, and touched upon the discussions of its interrelation with the rule of law. It is one of the few books dedicated entirely to profiling, however due to its time of publication, it does not make any reference to the form of political profiling nor does it explore the topic under the upcoming GDPR. Another piece of particular importance for my research has been the "Profiling Project- Protecting citizens' rights, fighting illicit profiling" (2014), a research project carried out by a consortium of five partners, among which the UN entity UNICRI and Tilburg University, which is focused on "identifying the challenges posed by the technology of profiling to the fundamental right to data protection".[20] Despite the fact that it constitutes a research among Switzerland and EU Member States' DPAs on the subject of automated profiling and does not offer any insight into political profiling, it proved to be a point of reference for my research as it built on previous research on the EU level. Still, by the time of the writing of the final report, the final text of the GDPR had not been adopted, so all relevant discussions on the topic were made with reference to the draft text

[19] Hildebrandt, M. and Gutwirth, S. (2008). *Profiling the European Citizen*. 1st ed. Dordrecht: Springer Science + Business Media B.V.

[20] Soziologe.guagnin.de. (2014). *PROFILING | PROtecting citizens' rights Fighting ILlicit profilING*. [online] Available at: http://soziologe.guagnin.de/profiling-project.eu/index.html%3Fp=6.html [Accessed 18 Dec. 2017].

of the Regulation.

Once the initial research on the topic of profiling was complete, my research moved to the concept of voters' privacy and regulation thereof. The article "Voter Privacy in the Age of Big Data" (I. S. Rubinstein, 2014) offers a comprehensive approach to the issue of micro-targeting voters for political communication, the privacy implications of such practice and its effect on democratic politics.[21] It offers insight, supported by research, on the data gathering and mining practices deployed by political parties, however it only touches upon the issue of their regulation in the US context. Nonetheless, considering that the academic literature on the matter is currently rather under-developed, this article is a welcome piece that functioned as the stepping stone for my research into the US profiling practices, regulation and discussions around the topic. The paper titled "Micro-targeting, Voter Intelligence and Data protection Law: Can Candidates and Political Parties Do in Europe What They Do in North America?" (C. Bennett, 2015) is the most recent of the publications that influenced my research and writing of this thesis, and is also the most relevant to my topic.[22] It provides an overview of the voters' micro-targeting practices in the US, Canada and Australia and the privacy risks associated with it, and it then proceeds to examine the issue in the European context. The article was edited in 2016 in order to include commentary on the GDPR, however it mainly focuses on the issue of profiling of voters in relation to Art. 9 of the Regulation, when the second chapter of this thesis analyses other provisions of the GDPR too, related to profiling and to the related rights granted to data subjects.

[21] Rubinstein, I. (2014). Voter Privacy in the Age of Big Data. *Wisconsin Law Review*. [online], pp.861-936. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447956 [Accessed 18 Dec. 2017].

[22] Bennett, C. (2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, [online] 6(4), pp.261-275. Available at: https://academic.oup.com/idpl/article/6/4/261/2567747 [Accessed 18 Dec. 2017].

Chapter 1: Voter data in the US and in EU: a brief overview

This chapter provides information on the sources of the voter data in the United States, the practices deployed by political parties when dealing with this data, with particular emphasis on the micro-targeting method and the privacy concerns associated with it. The regulatory framework surrounding these practices is briefly introduced and subsequently the European practices and EU regulatory framework are being briefly analysed respectively.

1.1 Voter data in the US

The latest Presidential elections in the United States created a heated debate and raised many questions regarding the use of individual voters' data by major political parties and candidates. The gathering of data about the electorate has a long history in the US, but the ever-growing vastness of the data gathered and the modelled and targeted manner it is being used for the communication to the electorate is new to its core. Major political parties, as well as marketing and big data analytics companies, have accumulated massive amounts of voters' data and have created national voter databases, in order to provide candidates with data to use during election campaigns and political races, from mayoral to presidential level.[23] There are numerous sources of this political data, the main body of which derives from local, state and federal records. These records include information such as party registration, donations to political parties, turnout records, but also real estate records and vehicle registration, among others. Other sources of political data include commercial information, which entails everything from credit card records to magazine subscriptions to even grocery stores "club-cards" purchases, but also driving records, criminal records, information about mortgages and gun-ownership.[24] Along with public and commercial data, generated information also constitutes part of the voter databases;[25] these databases are constantly merged and enriched with information regarding the "online identities and behaviour of voters".[26] This practically means that email sign-ups and

[23] Kreiss, D. (2012). Yes We Can (Profile You) A Brief Primer on Campaigns and Political Data. *Stanford Law Review*, [online] 66(70), p.71. Available at: https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/ [Accessed 18 Dec. 2017].

[24] Schipper, B. and Woo, H. (2017). *Political Awareness, Microtargeting of Voters, and Negative Electoral Campaigning*. [pdf] University of California, pp.2-3. Available at: http://faculty.econ.ucdavis.edu/faculty/schipper/polaw.pdf [Accessed 18 Dec. 2017].

[25] Kreiss, D. and Howard, P. (2010). New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era. *International Journal of Communication*, [online] 4, pp.1037-1038. Available at: http://ijoc.org/index.php/ijoc/article/view/870/473 [Accessed 18 Dec. 2017].

[26] Kreiss, supra note 23 at p.72.

information about “likes” and “friends” on Facebook, among others, are added to the voter databases.[27] The amount of personally identifiable information (PII)[28] that circulates on the Internet and is, in most cases, generated by the users, facilitates the building of voters’ profiles, who are targeted with political messages specifically built for and directed to them.[29] Marketing and big data analytics firms employed by major political parties use this data in order to create profiles, based on the different aspects of voters’ personal lives, in which information about their activities, place of birth, level of education, personal associations, type of work, commercial behaviour, religious beliefs and past political participation are also being added, along with others. [30] These profiles help predict in an accurate manner the voters’ behaviour, as discussed in detail below.

1.2 Micro-targeting and concerns associated with it

All this accumulated data is only meaningful in political campaigns when it is used in the context of a “voter model”, in the sense that it is tied in a significant way to the voters’ attitudes or behaviour.[31] The commonplace notion is, at least for the last decade, that political campaigns need to be “data-driven” in order for them to be successful and to attract more supporters and eventually more voters.[32] For this reason, political parties in the US

[27] Ibid.

[28] The term PII is commonly used in North America, however American privacy laws lack consensus on its definition. (Solove, D. and Schwartz, P. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, [online] 86(6), p.1827. Available at: http://heinonline.org/HOL/Page?handle=hein.journals/nylr86&div=50&g_sent=1&casa_token=&collection=journals [Accessed 19 Dec. 2017].) The term is often used by US government agencies, such as the National Institute of Standards and Technology (NIST) (SP 800-122), according to which “PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information”. PII can be considered as the European equivalent of “personal data” that is defined by the DPD and the GDPR as “any information relating to an identified or identifiable natural person (‘data subject’)”. According to the GDPR “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. It is evident that the definition of personal data covers a broader scope of information than this of the PII. In the text of this thesis the term PII is used, because it is the one used broadly in the US and the sub-chapter examines the US perspective of voters’ information collected and used for political communication purposes.

[29] Ca-political.com. (2017). *Services | CA Political*. [online] Available at: https://ca-political.com/services [Accessed 19 Dec. 2017]. See also supra note 15.

[30] Rustin-Paschal, N. (2011). Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues. *William & Mary Bill of Rights Journal*, [online] 19(4), p.922. Available at: http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1583&context=wmborj [Accessed 19 Dec. 2017].

[31] Kreiss, supra note 23 at p.71.

[32]Bennett, supra note 22 at p.261.

have invested heavily [33] during the past years in the construction of voters profiles, based on the amassed data, and in the "micro-targeting" of voters. Voter "micro-targeting", which is a term broadly used in the US, refers to the gathering of "*whatever individual-level information is available (i.e. IDs, vote history etc.) and combining thereof with demographic, geographic and marketing data about those individuals to build statistical models that predict the attitudes and behaviours of voters for whom that individual-level information is not known".*[34] It is considered to be one of the most valuable new technologies used for direct marketing in political campaigns,[35] which allows for highly personalised messages to be delivered to very particular segments of the electorate, using the most efficient means of communication, by applying "*predictive modelling techniques*" to the aforementioned voter databases. These personalised messages respond to the *"needs, wants, expectations, beliefs, preferences, and interests*" of the recipients, as they were determined by the analysis of the available data. [36] Notable is the view that micro-targeting "*enables candidates to focus their attention on issues that will help them win, irrespective of whether they are of concern to the broader electorate (…)*"[37], which emphasises the degree of personalisation of the political messages that voters receive. However, this has also been a point of critique, as it is questionable whether it allows for a public political debate to be created.[38] Public political debates are considered to be not only of paramount importance for the elections process alone, but also constitute "*the core of the concept of a democratic society*".[39] This latter point will be touched upon briefly below.

[33] Rubinstein, supra note 21 at p. 876.

[34] Definition taken by the site of Winning Campaigns, a Political Campaigns Management private organization. Winningcampaigns.org. (2017). *Winning Campaigns: Learn From The Experts Articles: Micro-Targeting: New Wave Political Campaigning*. [online] Available at: http://www.winningcampaigns.org/Winning-Campaigns-Archive-Articles/Micro-Targeting-New-Wave-Political-Campaigning.html [Accessed 19 Dec. 2017]. Micro-targeting is term similar to the term "profiling" used in the EU, in particular when it comes to its predictive character, however it differs to the part that it is not always automated (see definition of profiling in Article 4(4) GDPR).

[35] According to ICO the term direct marketing "is not limited to the offer for sale of goods or services only, but also includes the promotion of the aims and ideals of any organisation including political campaigns. This would include appeals for funds or support for a campaign, encouraging individuals to take some form of direct action or vote for a particular political party or candidate". Guidance on Political Campaigning. (2017). [ebook] ICO, p.5. Available at: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf [Accessed 19 Dec. 2017]. Cambridge Analytica lists digital marketing among the campaign components that help them deliver a successful full-scale data driven digital campaign, supra note 1. For more on the interrelation between direct marketing and political campaigns look at Chapter 2.4 of this thesis.

[36] Rubinstein, supra note 21 at p.882.

[37] Shipper, supra note 24 at p. 16

[38] Rubinstein, supra note 21 at p.910.

[39] Lingens v. Austria (1986) Series A no 103, para 42, ECtHR.

Although in the academic realms there seems to be some scepticism regarding the actual efficacy of the method of micro-targeting, as there is not enough evidence to support it, the world of political campaigns embraces it "wholeheartedly": not only it views it as effective, but also considers it to be of pivotal importance when it comes to determining the elections' outcome. This attitude probably originates from unpublished studies conducted by "*campaign insiders and paid consultants*"[40] and is most likely a sign that political actors will only keep on intensifying their efforts to accumulate even more voter data in the future. This annotation is the stepping stone to the following brief overview of the risks these data campaign practices bear and the points of criticism that have been underlined by academics.

There are a number of concerns that have been raised by academics and civil society regarding the threats that data-driven political campaigns pose to voters' privacy-related rights, although remarkable is the fact that, as already mentioned, the research on the topic remains rather under-developed to date.[41] On the one hand there are risks related to the voters' "information privacy", which is about the collection, use and disclosure of personal information, and is linked to the individuals' ability to exercise control over their data and personal information. On the other hand it has been observed that the ever-sophisticated technological tools that are being used for the marketing of political campaigns undermine the "political privacy", which refers to the "freedom to vote" and to "hold political discussions" and which is considered an imperative element for the democratic debate.[42]

Research has suggested that the methods used for the contemporary digital political campaigns are surrounded by a high degree of opacity:[43] the proliferation of data, along with the technologically advanced tools that are used to reveal the (online) behaviour of voters, makes it progressively more difficult for citizens to have control of their data and know what information about them is being collected and stored and by whom.[44] Adding to

[40] Rubinstein, supra note 21 at p.884.
[41] Bennett, supra note 22 at p.261.
[42] Rubinstein, supra note 21 at p.887.
[43] Kreiss, supra note 25 at p.1034.
[44] Berger, D. (2014). Balancing Consumer Privacy with Behavioral Targeting. *Santa Clara Computer and High Technology Law Journal*, [online] 27(3), pp.18-19. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1693029 [Accessed 19 Dec. 2017]. See also Gutwirth, S. and De Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.289,291. Available at: https://link.springer.com/book/10.1007/978-1-4020-6914-7 [Accessed 19 Dec.

that, political parties generally show unwillingness to reveal to the general public the practices that help them canvass voters.[45] It is evident that data practices for political campaigns purposes are characterised by a lack of transparency, which has also been a point of criticism for profiling and data mining practices in general.[46]

This lack of transparency, along with the inadequate regulatory framework for political data and voter micro-targeting in the US,[47] threaten a series of (information) privacy-related rights of voters; the extensive and ubiquitous nature of the gathering and processing of data nowadays leads, indeed, to individuals losing control of the information that is being collected about them and renders them unable to determine who this information is communicated to, if it is assumed that they were aware of it in the first place.[48] Amid claims that political data in the US is "traded on a largely unregulated and international market",[49] concerns regarding the "secondary use" of voter data are being raised; the numerous sources from which data can be drawn for political purposes makes it almost impossible for individuals to consent beforehand, especially when this data is transferred to third parties and/ or for commercial purposes, which is a common practice in the US.[50] Finally, the contingency of data breaches is always present, and highly publicised hacking incidents have occurred in the past,[51] so the feeling of insecurity that is being created to citizens who are subject to data campaigns is unshakable. With regard to political privacy, it has been

---

2017]. See also Borgesius, F. (2017). *Improving privacy protection in the area of behavioural targeting,* pp.115, 125. Ph.D. University of Amsterdam, Faculty of Law (FdR), Institute for Information Law (IViR).

[45] Kreiss, supra note 25 at p.1042.

[46] Schermer, B. (2011). *The limits of privacy in automated profiling and data mining*. [ebook] Computer Law & Security Review, Volume 27, Issue 1, pp.45-52. Available at: http://www.sciencedirect.com/science/article/pii/S0267364910001767 [Accessed 21 Nov. 2017]. See also Kuehn, A. and Mueller, M. (2012). *Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States*. [online], p.6. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181 [Accessed 19 Dec. 2017]. See also Gutwirth, S. and De Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.289. Available at: https://link.springer.com/book/10.1007/978-1-4020-6914-7 [Accessed 19 Dec. 2017].

[47] This will be examined in Chapter 1.3 of this thesis.

[48] van der Sloot, B. (2016). Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: S. Gutwirth, R. Leenes and P. De Hert, ed., *Data Protection on the Move*. [online] Dodrecht: Springer, p.430. Available at: https://link.springer.com/book/10.1007/978-94-017-7376-8#toc [Accessed 19 Dec. 2017].

[49] Kreiss, supra note 23 at p.73.

[50] Rubinstein, supra note 21 at p.868, 891, 914. See also Turow, J., Delli Carpini, M. X., Draper, N. A., & Howard-Williams, R. (2012). Americans Roundly Reject Tailored Political Advertising. Annenberg School for Communication, University of Pennsylvania, p.3. Available at http://repository.upenn.edu/asc_papers/ [Accessed 19 Dec. 2017].

[51] Goodin, D. (2013). *FBI warns hacking spree on government agencies is a "widespread problem"*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2013/11/fbi-warns-hacking-spree-on-government-agencies-is-a-widespread-problem/ [Accessed 19 Dec. 2017].

observed that it constitutes a fundamental value for the right to anonymous speech and freedom of association, but is compromised by the practices deployed during political campaigns, as described above, especially the voter micro-targeting, that renders it possible for the voters' beliefs and preferences to be constantly monitored online.[52] The high level of political messages' personalisation which is achieved with the help of voter micro-targeting, can also lead to behaviours that seriously deviate from the democratic ideal; campaigners can deliberately exclude big portions of the public, particularly the non-voters or those who are opposed to them, from receiving political messages,[53] leading to some form of "political redlining".[54] They can even "suppress turnout among specific sub-groups of voters",[55] by developing messages that play on their insecurities.[56] Additionally, micro-targeting enables candidates to highlight only the issues that will help them win, irrespective of whether they are issues of interest for the broader electorate, [57] or to address wedge issues that could be divisive when addressed in a more public forum. [58] Theoretically, politicians could even make contradictory promises to distinct groups of individuals. [59] It is eventually difficult to determine whether elected representatives are indeed representing the will of the people.[60] In such cases it is evident that the voting system becomes corrupted and the democratic procedure of elections is jeopardised.

These threats have not gone unnoticed from the electorate, as voters proceed to refrain from certain activities online in order to escape the "voter surveillance",[61] or even abstain from registering to vote, as they believe that this is the only way for their personal

[52] Rubinstein, supra note 21 at p.906. See also Ca-political.com. (2017). *Services | CA Political*. [online] Available at: https://ca-political.com/services [Accessed 19 Dec. 2017].
[53] Hillygus, D. and Shields, T. (2009). *The Persuadable Voter Wedge Issues in Presidential Campaigns*. Princeton: Princeton University Press, p.13.
[54] Howard, P.N. (2005). *New Media Campaigns and the Managed Citizen*. Cambridge University Press, p.131-142.
[55] Rubinstein, supra note 21 at p.908-909.
[56] Rustin-Paschal, supra note 30 at p.912.
[57] Hillygus, supra note 52 at p.13. See also Borgesius, F. (2017). *Improving privacy protection in the area of behavioural targeting,* p.125. Ph.D. University of Amsterdam, Faculty of Law (FdR), Institute for Information Law (IViR). See also Shipper, supra note 24 at p.16.
[58]Barocas, S. (2012). The price of precision: voter microtargeting and its potential harms to the democratic process. In: *Conference on Information and Knowledge Management*. [online] ACM, p.33. Available at: https://dl.acm.org/citation.cfm?id=2389671 [Accessed 19 Dec. 2017].
[59] Ibid.
[60] Hillygus, supra note 52 at p.13.
[61] Turow, J., Delli Carpini, M. X., Draper, N. A., & Howard-Williams, R. (2012). Americans Roundly Reject Tailored Political Advertising. Annenberg School for Communication, University of Pennsylvania, p.3. Available at http://repository.upenn.edu/asc_papers/ [Accessed 19 Dec. 2017].

information to remain private.[62] It is thus evident that profiling practices have a "chilling effect" on people, both as individuals and as voters, with relation to their online behaviour and voting patterns respectively.[63] Noteworthy is the fact that the majority of adult Americans reject tailored political advertising, because it deprives them of the control over their data, due to the lack of transparency of the techniques involved, and because they have not consented beforehand for the collection of their information for political advertising purposes.[64]

In the not so distant past, micro-targeting was achieved, as already mentioned, by applying "predictive modelling techniques"; these included the collective work of "analytic teams" and "statistical experts" who would study the data that had been collected, form test voters' groups based on these data, apply algorithms to the data in order to discover correlations or patterns linking individuals' characteristics with political beliefs, and lastly, apply this model to the larger voting population.[65] However, contemporary information technology has revolutionised the way micro-targeting is achieved nowadays; sophisticated algorithms and data mining tools have taken over, the human intervention part has been eliminated and the entire process has become totally automated.[66] This is the reason why most journalistic commentary (in lack of any academic thereof) on the 2016 US Presidential elections refers to "profiling" instead of micro-targeting.[67] The term "profiling" is further expanded on in Chapter 2 of this thesis.

The power that comes with the digitalisation of political campaigns is also highly advertised, by giant advertising platforms, like Google, that emphasise the "*unprecedented number of opportunities*" political campaigns have nowadays to *attract and persuade* voters online; as

[62] Rubinstein, supra note 21 at p.896

[63] Barocas, supra note 58, at p.34. For a definition of the "chilling effect" see van der Sloot, supra note 48 at p.422. For chilling effects as a privacy concern related to behavioural targeting in general see also Borgesius, F. (2017). *Improving privacy protection in the area of behavioural targeting,* pp.111, 115, 129, 183. Ph.D. University of Amsterdam, Faculty of Law (FdR), Institute for Information Law (IViR).

[64] Turow, supra note 61.

[65] Rubinstein, supra note 21 at pp.882-883. See also supra note 23 at pp.71-72.

[66] For the analysis of the term "automated" look at Chapter 2.2

[67] Doward, J. (2017). *Did Cambridge Analytica influence the Brexit vote and the US election?* [online] the Guardian. Available at: https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump [Accessed 20 Dec. 2017]. See also Davies, H. (2016). *Ted Cruz erased Trump's Iowa lead by spending millions on voter targeting*. [online] the Guardian. Available at: https://www.theguardian.com/us-news/2016/feb/01/ted-cruz-trump-iowa-caucus-voter-targeting [Accessed 20 Dec. 2017]. See also Funk, M. (2016). *Opinion | The Secret Agenda of a Facebook Quiz*. [online] Nytimes.com. Available at: https://www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html [Accessed 20 Dec. 2017].

they put it "*voters make decisions before they're in the booth- by going online*".[68] They also hind that the practices they use are "profiling" users; they offer targeted and tailored political advertisements that define voters' decisions in "micro-moments", when undecided individuals turn to their mobile devices.[69] "Targeted" refers to the analysis of voter data so it can be determined to whom, why and when a message should be sent, and "tailored" refers to the creation of persuasive messages based on the individual's preferences and interests as they were indicated by the targeting process.[70] It is supported by research that, under certain conditions, personalised or customised information makes the message more persuasive,[71] and it is claimed that micro-targeted messages are more persuasive and effective than other campaign communication means.[72] "Voter surveillance" is constant and political advertisements no longer target devices or particular sites, but the individual voter himself.[73]

1.3 International acknowledgement of the need for regulation

On an international level not much emphasis has been given on the regulation of the use of personal data for political communication purposes.[74] Back in 2005 the Data Protection Authorities (DPAs) around the world acknowledged the fact that political organisations started to take advantage of the new technologies and the newly available sources of information in order to establish personalised communication with the electorate. In the joint "Resolution on the Use of Personal Data for Political Communication" that they issued at their international conference in Montreux, they warned of "invasive profiling" and unlawful

[68] Think with Google. (2017). *What Marketers Can Learn From the Latest Data About Voter Behavior Online*. [online] Available at: https://www.thinkwithgoogle.com/consumer-insights/marketer-lessons-online-voter-behavior-data/ [Accessed 20 Dec. 2017].
[69] Think with Google. (2017). *How Political Ads and Video Content Influence Voter Opinion*. [online] Available at: https://www.thinkwithgoogle.com/marketing-resources/content-marketing/political-ads-video-content-influence-voter-opinion/ [Accessed 20 Dec. 2017].
[70] Turow, supra note 61, at p.3.
[71] Helberger, N. (2016). Policy Implications From Algorithmic Profiling and the Changing Relationship Between Newsreaders and the Media, *Journal of the European Institute for Communication and Culture,* [online] 23(2), p.193 Available at http://www.tandfonline.com/doi/full/10.1080/13183222.2016.1162989 [Accessed 20 Dec. 2017].
[72] Hillygus, supra note 52 at p.197.
[73] Maass, D. (2017). *Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election | Electronic Frontier Foundation*. [online] Available at: https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election [Accessed 20 December 2017].
[74] National electoral laws might regulate to a degree the processing of personal data used by campaigners and political parties for political communication purposes, however the investigation of such laws falls out of the scope of this thesis.

process of sensitive data related to political or voting activities.[75] They recognised that the aggressive means applied for the collection of large quantities of voters' data posed threats to individuals' information and political privacy and attempted to issue guidance on the matter by developing a worldwide minimum standard with which the processing of personal data for any political communication activity should comply. The data protection principles they suggested (among which these of the data minimisation, proportionality, consent of data subjects and the grant of particular rights to them) constitute an effort of the DPAs to contribute to the harmonisation of the levels of the protection of data subjects. However, only a few DPAs have seriously attempted to control the political organisations' practices in relation to political data.[76]

In 2013, the topic of profiling was in the centre of discussions among the data protection and privacy commissioners who adopted the "Resolution on profiling" during their international conference in Warsaw,[77] that reaffirmed the 2012 Uruguay's Declaration on Profiling.[78] The Resolution aimed to highlight the minimum data protection principles that should be taken into consideration when profiling practices are involved; among other points, particular emphasis was given on the transparency that should characterise profiling, namely the way profiles are assembled and the purposes for which these profiles are used. Transparency takes away privacy fears; it helps create trust among individuals regarding the profiling practices, reinforcing additionally their control over their data. A point of interest in both the Uruguay Declaration and the Resolution is the encouragement to avoid taking the human intervention out of the profiling process entirely, as the questionable (at the time) accuracy of its predictiveness could lead to injustice for individuals.

Although these Resolutions provide the minimum level of protection for the individuals' privacy and data protection related rights, they are purely suggestive; there are no legal

[75] Resolution on the Use of Personal Data for Political Communication. (2005). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf [Accessed 22 Dec. 2017].

[76] Bennett, supra note 22 at p.262.

[77] Resolution on profiling. (2013). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf [Accessed 22 Dec. 2017].

[78] Uruguay Declaration on profiling. (2012). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://edps.europa.eu/sites/edp/files/publication/12-10-26_uruguay_declaration_profiling_en.pdf [Accessed 22 Dec. 2017].

implications nor any sanctions can be imposed upon the countries that do not adopt them. It is up to each country to legally regulate its citizens' privacy and data protection rights.

1.4 Regulation of personal data used for political communication purposes in the US

The United States is "*the global pioneer on generating and storing political data*", however political campaigns and parties face almost no regulation with respect to the collection, use, storage and dissemination of citizens' data.[79] Profiling practices for political communication seem to have no legal implications whatsoever under the US privacy law:[80] there is no processing of personal data by any state authorities and they don't fall within the scope of the protection awarded by the Consumer Privacy Protection Act or any other privacy-related legislative piece.[81] Political entities generally enjoy great liberty when it comes to their data practices and the targeting of the electorate, mainly because it is considered that their restriction would be opposed to their freedom to speak to the citizens, which is protected by the First Amendment.[82] Lawmakers and courts widely protect parties and their candidates and grand them political exemption from federal laws, such as the Privacy Act, which even extents to the marketing and big data analytics companies employed by them.[83] Due to the absence of a complete and comprehensive information privacy law,[84] and because the "patchwork" of the various States' privacy regulations is inadequate to protect the individual voters,[85] the Federal Trade Commission (FTC) encourages companies that use individuals' personal data, towards the adoption of a self-regulatory regime.[86] The FTC has been urging

[79] Howard, P. and Kreiss, D. (2010). Political parties and voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective. *First Monday*, [online] 15(12), p.21. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595120 [Accessed 22 Dec. 2017].

[80] Zanfir-Fortuna, G. (2016). *A look at political psychological targeting, EU data protection law and the US elections*. [online] pdpEcho. Available at: https://pdpecho.com/2016/11/14/does-eu-data-protection-law-apply-to-the-political-profilers-targeting-us-voters/ [Accessed 22 Dec. 2017].

[81] Ibid.

[82] Kreiss, supra note 25 at p.1039. For the wording of the First Amendment look at LII / Legal Information Institute. (2017). *First Amendment*. [online] Available at: https://www.law.cornell.edu/constitution/first_amendment [Accessed 22 Dec. 2017].

[83] Howard, Kreiss, supra note 79 at pp.1040-1041.

[84] Rubinstein, I., Lee, R. and Schwartz, P. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review*, [online] 75(1), p.273. Available at: http://scholarship.law.berkeley.edu/facpubs/1497/ [Accessed 22 Dec. 2017].

[85] Bennett, supra note 22 at p.274.

[86] Rustin-Paschal, supra note 30 at p.921. See also Staff Report (2009). *Self-regulatory Principles for online behavioral advertising*. [pdf] Federal Trade Commission, pp.11-12. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [Accessed 22 Dec. 2017].

companies towards self-regulation since 1998,[87] and continuously issues guidance in the area of online behavioural advertising, advising companies to adopt a set of principles, that guarantee transparency and control for the data subjects, limitations to the retention of data and expressed consent when changes happen to privacy policies as well as when sensitive data is used for advertising.[88] Unfortunately, most state voting laws fail to satisfy even those minimum requirements.[89] The industry has responded with self-regulatory frameworks.[90] However, these principles constitute mere recommendations and are not enforceable by law, meaning that the monitoring and enforceability of the self-regulation should be the goal of the industry, so that this self-regulation scheme becomes effective.[91] This is the reason why FTC recommends that the US Congress enacts legislation, which along with the self-regulation will provide sufficient protection for the citizens' privacy and data protection-related rights.[92] It should also be noted that FTC has excluded all non-advertising behavioural targeting from the principles' applicability scope.[93] Regarding the voter suppression that can be achieved with the means of highly targeted and tailored political advertising, as has already been analysed to a certain extent,[94] there is no federal law that protects the voters, and any effort that has been done to fill this legislative gap has been proven to be unsuccessful.[95] In the absence of any government regulation on the subject, voter data might be "*the largest concentration of unregulated personal information in the US today*".[96]

[87] Online Profiling: A report to Congress. (2000). [pdf] Federal Trade Commission, pp.17-22. Available at: https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress/onlineprofilingreportjune2000.pdf [Accessed 22 Dec. 2017].

[88] Rustin-Paschal, supra note 30 at p.921. See also Berger, D. (2014). Balancing Consumer Privacy with Behavioral Targeting. *Santa Clara Computer and High Technology Law Journal*, [online] 27(3), p.5. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1693029 [Accessed 22 Dec. 2017]. See also Staff Report (2009). *Self-regulatory Principles for online behavioral advertising*. [pdf] Federal Trade Commission, pp.11-12. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [Accessed 22 Dec. 2017].

[89] Rubinstein, supra note 21 at p.869.

[90] Supra note 87 at pp.17-22.

[91] Rustin-Paschal, supra note 30 at p.921.

[92] Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. (2000). [pdf] Federal Trade Commission. Available at: https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission [Accessed 22 Dec. 2017].

[93] Berger, D. (2014). Balancing Consumer Privacy with Behavioral Targeting. *Santa Clara Computer and High Technology Law Journal*, [online] 27(3), p.44. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1693029 [Accessed 22 Dec. 2017].

[94] Look at Chapter 1.2 of this thesis.

[95] Rustin-Paschal, supra note 30 at pp.915-916.

[96] Rubinstein, supra note 21 at p.881.

1.5 Regulation of personal data used for political communication purposes in the EU and applicable data protection law

While "voter surveillance" is not nearly as extensive or sophisticated in other countries as is in the US, political parties and candidates around the world, and Europe, have reportedly long coveted the practices deployed by their US counterparts and wish for similar abilities in an effort to attract more supporters and eventually voters.[97] It should be noted however, that there are pivotal differences between the presidential system in the US and the parliamentary systems that exist in Europe, and there are a number of reasons for which it has been argued that this American experience cannot be fully realised into the European grounds.[98] Despite the differences that could hinder the import of the US practices in EU, there is evidence that similar techniques are currently entering Europe's political system.[99] Big data analytics companies and political consultants, who wish to benefit to the maximum from data-driven campaigns and micro-targeting, are more than willing to share their know-how on the subject; transnational communication on the matter is reportedly already extensive.[100]

Political advertising and its practices seem to have gone mostly unmonitored and escaped public scrutiny and debate, especially in Europe, at least until recently,[101] with a few recent exceptions from investigative journalism; it is claimed that during the political campaign for Brexit alone, billions of UK pounds were invested in digital advertising and nearly a billion of targeted adds were sent to individual voters, in an attempt to influence their votes.[102]

[97] Hillygus, supra note 53 at p.195.

[98] Bennett, supra note 22 at p.274. According to Professor C. J. Bennett the US is different from other democratic countries because of the liberal campaign finance laws, the decentralized two-party system that permits much local autonomy, the polarized political system that encourages a competitive race for increasingly sophisticated data mining and analytical tools, the First Amendment that defines campaign contributions as "speech", the widespread commercial market in personal data and the absence of any comprehensive data privacy law.

[99] Bennett, C. (2013). The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. *First Monday*, [online] 18(8). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4789 [Accessed 22 Dec. 2017].

[100] Rubinstein, Lee, Schwartz, supra note 84 at p.261.

[101] ICO only announced that they are launching an investigation regarding profiling practices deployed by campaigners for political communication purposes in 2017 and it is seemingly the first effort for an official investigation of the topic in EU grounds.

[102] McClenaghan, M. (2017). *The "dark ads" election: How are political parties targeting you on Facebook?*. [online] The Bureau of Investigative Journalism. Available at: https://www.thebureauinvestigates.com/stories/2017-05-15/the-dark-ads-election-how-are-political-parties-targeting-you-on-facebook [Accessed 22 Dec. 2017]. See also Major, K. (2017). *Facebook 'dark ads' will win this election for the Tories - but there's something you can do about it*. [online] The

France is claimed to have started heavily investing in digital political campaigning as well,[103] but none official investigation has been conducted so far on the matter from any EU DPA or any other independent authorities, with the exception of UK's Information Commissioner's Office that announced the launching of investigation into the online targeting of voters from political parties and candidates, as already mentioned.[104]

Subsequently, the current regime for political data and its regulation in the EU is examined. As far as voters' databases are concerned, it should be noted, that apart from the UK, whose management of the databases is similar to this of the US, the handling of voters' data by political parties in the rest of the European countries is typically surrounded by secrecy.[105] Europe, however, has a more comprehensive data protection system and legislation than the US. The processing of personal data is currently regulated by the Data Protection Directive (DPD) which came into force in 1998 and constitutes the basic EU data protection instrument.[106] Political parties and the marketing firms that work for them are covered by the Directive, when they collect and process voters' personal information; nevertheless the wording of the Directive has many ambiguities and vague notions when it comes to terms such as "political opinions" and "electoral activities", and not much guidance has been given regarding their interpretation.[107] The Directive is succeeded by the General Data Protection Regulation (GDPR) which is coming into force in May 2018.[108] The GDPR

Independent. Available at: http://www.independent.co.uk/voices/election-facebook-dark-targeted-ads-tories-labour-do-something-a7745341.html [Accessed 22 Dec. 2017].

[103] Supra note 10.

[104] Supra note 11.

[105] Bennett, supra note 22 at p.268.

[106] 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, OJ L 281, 23/11/1995, pp.0031-0050.

[107] Bennett, supra note 22 at pp.266-267.

[108] 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), OJ L 119, 04/05/2016, pp.1-88.
Although the Directive was introduced in order to address the differences in national laws and create a uniform legislation on a European level that would safeguard citizens' personal data protection, it appears that ultimately, the desired harmonisation was not fully achieved. Different national interpretations on fundamental concepts of the Directive, issues regarding the interrelation with the national law as well as the Directive's applicability in each Member State's market, and finally the DPAs' latitude in adopting enforcement measures, were a few of the factors that led to the calling for replacement of the Directive with a European regulation directly applicable to all Member States; (Poullet, Y. (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review*, [online] 22(3), pp.206-217. Available at: https://www.sciencedirect.com/science/article/pii/S0267364906000318 [Accessed 22 Dec. 2017]). The Regulation is directly applicable to all Member States' national legislations, achieving the highest possible level of uniformity and harmonization of the law in the European Union. The GDPR marks a milestone in European data protection law and is considered the most significant legislation since the adoption of the Directive. It

sets obligations for increased transparency, more information to be provided to individuals when it comes to their rights to access their data and be informed about their uses, and most importantly it explicitly regulates profiling.[109]

Although the provisions of the GDPR regarding profiling will be thoroughly analysed and examined in the second chapter of this thesis, the reasoning behind the regulation thereof will be briefly presented here; the GDPR poses serious restrictions on the ways profiling can be conducted, acknowledging its widespread application in recent years with the help of the enormous amounts of interconnected data that are being available each day.[110] Much of the terminology used in the text of the Regulation is unclear and the practical implementation of these provisions might be proved to be a hard task. The Art.29WP[111] issued in October 2017 its much anticipated guidelines on automated individual decision-making and profiling, [112] for the purposes of the GDPR, providing some clarifications on the respective provisions. The provisions of the Directive, for which it has been claimed that they lack any particular "*concerns about the technology*", are rendered outdated, by the ever-advancing technological aspects of practices such as profiling, which were in their infancy when the final text of the Directive was adopted. This is probably the main reason

---

has been characterised as a "Copernican Revolution", and attempts to revolutionise the protection offered to individuals, by providing them with a high level of control over their data while increasing data controllers' obligations respectively; Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781 [Accessed 2 Jan. 2018].

[109] De Hert, P. and Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, [online] 28(2), p.136. Available at: https://www.sciencedirect.com/science/article/pii/S0267364912000295 [Accessed 22 Dec. 2017].
Profiling (and automated decision-making) are also covered by Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119.

[110] European Data Protection Regulation: Information Sheet. (2016). [ebook] Privacy Europe, p.12. Available at: https://www.privacy-europe.com/blog/wp-content/uploads/2016/03/European-Data-Protection-Regulation-Information-Sheet.pdf [Accessed 22 Dec. 2017].

[111]The Article 29 WP is "the establishment of a consultative and independent Committee working close to the Commission that joins together representatives of the different national Data Protection Authorities, responsible for submitting advice and recommendations to the European institutions on specific privacy issues"; Poullet, Y. (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review*, [online] 22(3), p.208 Available at: https://www.sciencedirect.com/science/article/pii/S0267364906000318 [Accessed 22 Dec. 2017].

[112] Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 3 October 2017. WP251. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 22 Dec. 2017].

why it was deemed necessary for it to be replaced by the Regulation that, at least at first sight, seems to have taken such matters into consideration.[113]

The processing of personal data by political parties and candidates, which falls within the scope of the GDPR, as will become evident from the next chapter of this thesis, has not been raised during the debates before the adoption of the final text of the Regulation, and as already noted, the limited criticism of the provisions regarding profiling is focused on the complexities of their implementation in practice. However, as the US profiling practices enter into the European political environment, it is expected that this topic will be the subject of many discussions in the near future and a higher level of clarification by the European instruments will be deemed necessary.

1.6 Conclusion

Extensive profiling practices for political campaigns are increasingly becoming the new norm in the United States, however they remain vastly unregulated for a number of reasons, leaving voters' online privacy susceptible to breaches. The lack of transparency surrounding the data practices of campaigns and the subsequent lack of the individuals' control over their data, have been the main points of concern and criticism. On the other hand, in Europe, where the US practices are being slowly (?) transferred into the Member States' political systems, having seemingly escaped public attention, the legal frameworks- both existing and upcoming, promise high safeguards related to individuals' privacy and data protection rights. The GDPR was especially drafted to provide, through increased transparency, the highest level of control to individuals with regard to their data, although the Regulation's effectiveness has not yet been tested to practice. On the next chapter the extent to which the Regulations' provisions regarding profiling, within the scope of political campaigns activities will be examined, in addition to whether these are indeed living up to the high expectations that were set by this new legislation.

[113] Poullet, Y. (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review*, [online] 22(3), p.216. Available at: https://www.sciencedirect.com/science/article/pii/S0267364906000318 [Accessed 22 Dec. 2017]. See also Skouma, G. and Léonard, L. (2015). On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. In: S. Gutwirth, R. Leenes and P. de Hert, ed., *Reforming European Data Protection Law*. [online] Dordrecht: Springer, p.36. Available at: https://link.springer.com/chapter/10.1007%2F978-94-017-9385-8_2 [Accessed 22 Dec. 2017].

Chapter 2: Political profiling and its regulation under the GDPR

This chapter provides an overview of non-legal definitions of profiling, followed by its legal definition under the GDPR, it explores the concept of behavioural profiling and its interrelation to political profiling, it examines whether the right to object and the right not be subject to automated decision-making are attributed to political profiling subjects by the GDPR and finally weighs in on the exceptions provided by Article 9 (2) GDPR and their impact on the individuals' protection by the Regulation.

2.1 Introduction to the concept of profiling: overview of non-legal definitions

"*A powerful technique that renders visible what is invisible to the naked human eye*".[114]

Profiling has lately become a catchword and the buzz around it only keeps on growing as there is a constant proliferation of new, data-driven, digital technologies. Although this term is not new in the industries of marketing and advertising, its application in the area of political campaigns, where users' data does not reveal a product preference, but a political one, remains rather unexplored. This is a complicated and rapidly expanding area of activity, yet the level of awareness among the public regarding the profiling practices deployed by major political parties is really low. For campaigners maintaining a secrecy around the topic is a matter of maintaining competitiveness.[115] But how is profiling defined?[116]

Profiling has multiple meanings and the term is used in both specialist and non-specialist contexts.[117] It is notable that in the academic literature not many definitions exist for

[114] Hildebrandt, M. (2017). Who is Profiling Who? Invisible Visibility. In: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne and S. Nouwt, ed., *Reinventing Data Protection?*. [online] Dodrecht: Springer, p.241. Available at: https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_14 [Accessed 22 Dec. 2017].
[115] Barocas, supra note 58 at p.34.
[116] For a general discussion on profiling and the legal challenges associated with it, see Bygrave, L. (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Report*, [online] 17, pp.17-24. Available at: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf [Accessed 22 Dec. 2017]; Dinant, J.M., Lazaro, C., Poullet, Y., Lefever, N. and Rouvroy, A. (2008). Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD), Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, 11 January, Strasbourg; and Hildebrandt, M. and Gutwirth, S. (2008). *Profiling the European Citizen*. 1st ed. Dordrecht: Springer Science + Business Media B.V.
[117] Bosco, F., Creemers, N., Ferraris, V., Guagnin, D. and Koops, B. (2015). Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. In: S. Gutwirth, R. Leenes and P. de Hert, ed., *Reforming European Data Protection Law*. [online] Dodrecht: Springer, p.5. Available at: https://link.springer.com/chapter/10.1007/978-94-017-9385-8_1 [Accessed 22 Dec. 2017].

profiling. Generally profiling is perceived as a data mining method: it is a (semi-) automated process with which large data sets are examined in order to form categories of characteristics.[118] One of the oldest definitions of profiling is attributed to Gary T. Marx, who gave particular emphasis to the logic behind profiling and connected it to the law enforcement domain,[119] while Roger Clarke defined it as a "*dataveillance technique (…)*".[120] One of the best efforts to accurately define profiling and its features is credited to Mireille Hildebrandt, who defines it as follows: "*the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/ or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify a subject as a member of a group (which can be an existing community or a discovered category)*".[121] She additionally underlines the importance of prediction when she describes profiling as the "*discovery of patterns that present knowledge which enables anticipation of future events based on what happened in the past*".[122] The predictive character of profiling is also emphasized in the European Commission's INEX project paper regarding profiling in the European Union, where it is referred to as "the use of predictive data mining to establish recurrent patterns or 'profiles' permitting the classification of individuals into different categories".[123] The profiling process has two main constituents: the profile generation and the profile application, meaning the process of creating a profile based on the gathered data and the process of making a decision about a person based on the generated profile respectively. In practice however it

[118] Ibid. at p.4.

[119] Marx, G. (1984). Routinizing the Discovery of Secrets- Computers as Informants. *American Behavioral Scientist*, [online] 27(4), p.429. Available at: http://journals.sagepub.com/doi/abs/10.1177/000276484027004003#articleCitationDownloadContainer [Accessed 22 Dec. 2017].

[120] Clarke, R. (1993). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law and Information Science*, [online] 4(2). Available at: http://heinonline.org/HOL/Page?handle=hein.journals/jlinfos4&div=33&g_sent=1&casa_token=&collection=journals# [Accessed 22 Dec. 2017].

[121] Hildebrandt, M. (2009). Profiling and AmI. In: K. Rannenberg, D. Royer and A. Deuker, ed., *The Future of Identity in the Information Society*. [online] Berlin: Springer, p.275. Available at: https://link.springer.com/chapter/10.1007/978-3-642-01820-6_7 [Accessed 22 Dec. 2017].

[122] Ibid. at p.289.

[123] González Fuster, G., Gutwirth, S. and Ellyne, E. (2010). *Profiling in the European Union: A high-risk practice*. [ebook] INEX POLICY BRIEF NO. 10, p.2. Available at: https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf [Accessed 22 Dec. 2017].

is rather difficult to distinguish between the two processes.[124] Profiling is generating knowledge and provides new forms for the applying thereof.[125]

Due to the ever expanding capacities of databases, the analysis of the data collected through profiling procedures becomes increasingly complex and sophisticated, thus the role of humans in this process is significantly affected. Accordingly, profiling can be either non-automated, which by definition does not rely on any process of automation, or automated, which involves automation technologies that process data and reach to decisions without the intervention of human knowledge. Automated profiling is defined by the "PROFILING - PROtecting citizens' rights and Fighting ILlicit profilING" project as the "automated processing of data to develop predictive knowledge in the form of profiles that can subsequently be applied as a basis for decision-making".[126]

All the aforementioned definitions were formed, in lack of a harmonised legal definition, in order to fill the legislative gap and be used as a basis for explanation and analysis of the profiling technique and its interrelation with legally protected rights.

Before the GDPR, there had been an effort to define profiling in the European context from a data protection perspective with the Council of Europe Opinion (CoE Recommendation) on profiling, according to which profiling is an "*automated data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*".[127] However, this Recommendation is not legally binding and none of the Member States implemented it.[128]

[124] Bygrave, L. (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Report*, [online] 17, p.18. Available at: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf [Accessed 22 Dec. 2017].
[125] Bosco, Creemers, Ferraris, Guagnin, Koops, supra note 117 at p.7.
[126] PROtecting citizens' rights and Fighting ILlicit profilING (PROFILING) project (2014). *Profiling- Protecting citizen's rights, fighting illicit profiling*. [online] p.vi. Available at: http://www.unicri.it/news/files/Profiling_final_report_2014.pdf [Accessed 22 Dec. 2017].
[127] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). Available at: http://194.242.234.211/documents/10160/10704/Recommendation+2010+13+Profiling.pdf
[128] PROFILING project, supra note 126 at p.19.

2.2 Definition of profiling under the GDPR

Profiling is currently regulated by the DPD. Although the term "profiling" is not explicitly mentioned in the text of the Directive and no particular measures regarding profiling are foreseen, Article 15 DPD regulates the processing of personal data with automated means, which is linked to profiling. Before the GDPR, most Member States' DPAs considered it essential for a legal definition on automated profiling to be adopted,[129] in order for its concept and the procedures used to be illuminated. Only three countries had adopted a legal definition on profiling (on a national level), before the Regulation, which, as already mentioned, provides a harmonised legal definition of profiling.[130]

Article 4 (4) GDPR defines it as "*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*".[131]

The term "profiling" appears several times in the text of the Regulation and is particularly linked to Article 22, titled "*Automated individual decision-making, including profiling*". The GDPR, however, does not cover only the decisions made as a result of automated processing or profiling, but also applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals or groups of individuals.[132] Article 22 (1) GDPR states that "*the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, (…)*". The word "solely" is absent from the definition given in Article 4 (4) GDPR, and thus the question what "automated processing" means, arises. According to Art.29WP, profiling has to involve some form of automated processing, however human involvement does not take the activity out of the definition.[133] This interpretation is contrary to Hildebrandt's interpretation and distinction between two forms of profiling, the "autonomic" and the "automated" one, the latter of which

[129] Bosco, Creemers, Ferraris, Guagnin and Koops, supra note 117 at p.23.
[130] PROFILING project, supra note 126 at p.14.
[131] Article 29 WP notes in their Guidelines on Automated individual decision-making and Profiling (p.7) that the GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec (2010) 13, as the Recommendation excludes processing that does not include interference.
[132] Art.29WP, supra note 112 at p.6.
[133] Ibid.

includes human intervention that takes the processing out of the provision's applicability scope.[134]

Despite the fact that the need for the legal definition of profiling was born due to the extremely fast-developing information society, the ever-advancing technologies and sophisticated methods with which profiling can be achieved, and the fact that most profiling techniques seem to be rather advanced from a technological point of view and to lack the "human intervention" factor, the interpretation given by Art.29WP, covers all profiling practices and offers a broad range of protection for the profiling subjects. There are indeed cases where it appears rather unrealistic for a human to intervene in the processing of the vast amounts of data that are being available each day and are being deployed for profiling purposes, however Art.29WP made sure that the appropriate safeguards for the protection of the rationale[135] of the Regulation are provided; companies could deploy essentially "autonomic" profiling, but have a human intervene in a rather unimportant part of the processing, undermining and eventually rendering void the applicable provisions of the Regulation, depriving at the same time individuals from the protection guaranteed by it.

According to Article 4 (4), the processing of data is used for the purposes of *evaluation of certain personal aspects* of the data subjects, in particular to *analyse or predict* those aspects. Since there is a distinction between the analysis and the prediction of personal aspects, this could be interpreted to mean that personal aspects of natural persons could be analysed, either by previously known data, already available to the processor, or by newly acquired data through the processing or to be used for the prediction of their behaviour in order to make a decision about them. So companies could use data that is

[134] Hildebrandt's distinction refers to the DPD, and is only mentioned here because of its relevance with the GDPR: according to Hildebrandt, autonomic profiling is done solely by a "network of machines that processes data, constructs knowledge and makes decisions without the intervention of a human consciousness". For the automated profiling she gives the example of profiles that are "generated and applied in the process of data mining, after which human experts sit down to filter the results before making decisions". Accordingly, she claims that any form of routine human intervention renders Art.15 of the DPD not applicable (Art. 15 of the DPD has a similar wording to Art. 22 of the GDPR and is as follows: "*every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc*."). Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge?. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, p.28. Available at: https://link.springer.com/chapter/10.1007/978-1-4020-6914-7_2 [Accessed 22 Dec. 2017].

[135] Besides the harmonisation of data privacy laws across Europe, the GPDR also aims to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. More on: EU GDPR Portal. (2017). *Home Page of EU GDPR*. [online] Available at: https://www.eugdpr.org/ [Accessed 22 Dec. 2017].

being directly provided by their customers, or combine this with data available from a previous time.[136] Art.29WP concluded that this distinction also means that solely assessing or classifying individuals based on their characteristics, without any predictive purpose, could also be considered profiling.[137] This interpretation takes away the predictive nature of profiling that has been emphasised by legal academics.[138]

Given the core principle of transparency underpinning the GDPR, controllers are obliged to explain to individuals in a clear and simple manner how profiling and automated decision-making works.[139] Recital 60 of the GDPR states that "*the data subject should be informed of the existence of profiling and the consequences of such profiling*". Recital 63 states that every data subject should have the right to know and obtain communication with regard to "*the logic involved in any automatic personal data processing and, at least, when based on profiling, the consequences of such processing*".[140] It is clear that both Recitals emphasise the fact that the consequences of profiling should be communicated to the data subjects, apart from the fact that individuals should be explicitly informed that they are subject to profiling. Recital 68 aims at further empowering the data subjects by allowing them to receive personal data concerning them or data that was provided to the controller "*in a structured, commonly used, machine-readable and interoperable format*"[141] where the processing of their data is carried out by automated means, in order to transmit it to a different controller.

2.3 Behavioural profiling in the form of political profiling

Recital 24 of the GDPR, which is associated to Article 4 (4), provides that "(…) *in order to determine whether a processing activity can be considered to* ***monitor the behaviour*** *of data subjects, it should be ascertained whether natural persons are tracked on the internet*

[136] Feedback request – profiling and automated decision-making. (2017). [ebook] Information Commissioner's Office, p.8. Available at: https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf [Accessed 22 Dec. 2017].
[137] Art.29WP, supra note 112 at p.7.
[138] See Chapter 2.1 of this thesis.
[139] Look at Articles 13 (2) (f) and 14 (2) (g) GDPR as well as Recitals 39, 58 and 60.
[140] According to Art.29WP251 guidelines, the right of the data subject to obtain meaningful information about the "logic involved" means that the controller should find simple ways to inform the data subject about the rationale behind, or the criteria relied on in reaching the decision without necessarily always trying to provide a complex explanation of the algorithms used or disclose the full algorithm. Complexity is no excuse for failing to provide information to the data subject. The view that only information regarding the rationale should be provided, and none of a "decompositional nature", has been a point of critique. See Infra note 165.
[141] Also look at Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679. WP 260, p.22. Available at ec.europa.eu/newsroom/document.cfm?doc_id=47741.

including potential subsequent use of personal data processing techniques which consist of ***profiling a natural person****,* ***particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes***".

The "monitoring of behaviour" refers to the concept of "behavioural profiling" (also known as "targeting", "micro-targeting"[142] or "behavioural targeting"[143]), which is the study of patterns of behaviour of individuals and their subsequent grouping in categories according to the behaviours that have become apparent. The most common application of behavioural profiling today is the one on online users.[144] When profiling users online, several data points, attributable to a single originating entity, are collected and analysed (with the help of data mining algorithms) in order to acquire knowledge relating to this entity.[145] The more information is obtainable, the more potential profiling has.

Is political profiling a form of behavioural profiling? In order for this question to be answered, a brief definition of political profiling is imperative at this point: for the purpose of this thesis, political profiling encompasses profiling deployed by political parties in the course of their elections campaigns, which aims at revealing voters' political opinions and preferences. For the definition of political campaigns and political parties see Chapter 2.4 of this thesis.

According to the aforementioned, it could most likely be considered to be a form of behavioural profiling; there has been an increasing tendency among major political parties to send data-driven messages during the period of election campaigns. Elections management agencies that collect and process personal data for the purposes of building voters profiles, gather data from posts or likes on Facebook or other social media, visits on popular websites that reveal preferences for food and clothing, car ownership, state of health etc., even from apps that keep political supporters in touch, while scrapping at the

[142] Castelluccia, C. (2012*). Behavioural Tracking on the Internet: A Technical Perspective*. In: S. Gutwirth, ed., European Data Protection: In Good Health?,. Springer.
[143] Borgesius, F. (2017). *Improving privacy protection in the area of behavioural targeting*. Ph.D. University of Amsterdam, Faculty of Law (FdR), Institute for Information Law (IViR).
[144] AMAPOLA, UNICRI, Tilburg University (2014). *Defining Profiling*. [online] p.10. Available at: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf [Accessed 22 Dec. 2017].
[145] Castelluccia, supra note 142 at p.22.

same time the smartphone for additional information, such as contacts and so on.[146] All this data is processed in a way that creates "enhanced voter files", containing up to dozens of thousands of data points per person.[147] Personality traits models, traditionally used by psychologists to describe the human personality and psyche, are applied in order to create such profiles, with the ultimate goal being this of the creation of specific ad messages, tailored to those profiles.[148] The level of personalization of the ads is extremely high, as, depending on the recipient, differences in the headings, colours, captions or photos can apply;[149] ads are crafted in a way that engages voters "emotionally and impactfully".[150] With techniques such as "geo-fencing"[151] even the smallest groups can be targeted, from a city block, to a single building, to particular individuals.[152]

Political profiling is therefore a type of profiling the regulation of which falls within the scope of the GDPR. What remains to be explored is the rights that individuals, who are subjects to political profiling practices, are granteded by the Regulation. Particularly, the main focus of the analysis will be this of the right to object and the right not to be subject to automated decision making, which are both linked to the profiling practices.

2.4 Political campaigns as direct marketing and the right to object

The first right related to profiling is the right to object. The first paragraph of Article 21 of the Regulation provides that "*the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR,[153] including profiling based on*

[146] Hamburger, T. (2015). *Cruz campaign credits psychological data and analytics for its rising success*. [online] The Washington Post. Available at: https://www.washingtonpost.com/politics/cruz-campaign-credits-psychological-data-and-analytics-for-its-rising-success/2015/12/13/4cb0baf8-9dc5-11e5-bce4-708fe33e3288_story.html?utm_term=.d4ac51b9e4c8 [Accessed 22 Nov. 2017].
[147] Ibid.
[148] Kaye, K. (2016). *In D.C., Cambridge Analytica Not Exactly Toast of the Town*. [online] Adage.com. Available at: http://adage.com/article/campaign-trail/cambridge-analytica-toast/305439/ [Accessed 22 Nov. 2017]. For the "enhanced voter file" see also: Barocas, supra note 58 at p. 32.
[149] Grassegger, H. and Krogerus, M. (2017). *The Data That Turned the World Upside Down*. [online] Motherboard. Available at: https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win [Accessed 22 Nov. 2017].
[150] Look at the targeted advertising section at: Ca-political.com. (2017). *Services | CA Political*. [online] Available at: https://ca-political.com/services [Accessed 22 Dec. 2017].
[151] WhatIs.com. (2017). *What is geo-fencing (geofencing)? - Definition from WhatIs.com*. [online] Available at: http://whatis.techtarget.com/definition/geofencing [Accessed 22 Dec. 2017].
[152] Grassegger and Krogerus, supra note 149. See also: Hamburger, supra note 145.
[153] Article 6 GDPR provides the legal grounds for processing personal data.

those provisions (…)", and the second paragraph particularly gives this right to data subjects in the cases where personal data is processed for direct marketing purposes: "*where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing*". The second paragraph grants an unconditional right to the data subjects, meaning that the controller must respect the individual's wishes without questioning the reasons for objection.[154] The right to object based on the second paragraph is absolute, according to the third paragraph. This means that once the individual exercises this right, the controller must interrupt[155] the profiling process and might also need to erase all relevant data.[156] According to Recital 70, the data subject has the right to object whether with regard to initial or further processing, not only at any time, but also free of charge. The data subject should be explicitly informed about this right of his or hers, which should also be presented in a clear manner and be distinguishable from any other information. It is obvious that emphasis has been given to the facilitation of the individual to exercise this right.

It should first be explored whether political parties could base their profiling practices on either point (e) or (f) of Article 6 (1) GDPR.[157] Based on Recital 56 that states that "*where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established*", it could be claimed that profiling practices deployed by political parties are conducted for reasons of public interest. In such a case, the profiling subjects could base their right to object on Article 21 (1) GDPR however the controller could demonstrate *compelling legitimate grounds* for the processing, which overrides the interests or rights and freedoms of the data subject. The burden of proof to demonstrate legitimate grounds lies with the controller. According to Art.29WP a balancing

[154] On the contrary, according to WP 251, when the data subject objects to profiling that is not done for direct marketing purposes (Article 21 (1) GDPR), the controller could reply by demonstrating compelling legitimate grounds that override the rights and freedoms of the data subject. A balancing between the interests of the controller and the basis for the data subject's objection should be achieved in that case.
[155] Article 18 (1) (d) GDPR.
[156] Article 17 (1) (c) GDPR.
[157] Article 6 (1) (e) GDPR processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (…).

of interests of the controller and the basis for the data subject's objection should be achieved in this case; the controller should prove that profiling is the least intrusive method to achieve his particular objectives, and that the objective is critical for the organisation. What this practically means is that, since political parties have a greater power than individuals, they could conduct researches that would serve their best interests on the matter, presenting political profiling as less intrusive and privacy-threatening than academics and legal scholars claim it to be. Consequently, when the right to object to political profiling is based on Article 21 (1) GDPR, it could possibly be overridden by political parties.

Assuming that the safeguards for individuals are higher when exercising their right to object based on Article 21 (2) GDPR, it should be explored whether profiling subjects can base their right on it. What is of particular relevance here is the term "direct marketing". It should be explored whether the term "political campaign" falls under the term "direct marketing", in order for this right to be attributable to individuals who are subject to political profiling. For the purpose of this thesis, the term "political campaigns" encompasses generally the activity to support and promote or be against a political party or a candidate during elections. The term "political parties" broadly covers individuals, such as candidates, employees or volunteers, and organisations or companies that work for such political campaigns purposes.[158]

ICO states that promotion of political parties' vision and opinions through their campaigns constitutes marketing.[159] However, what is of importance is the direct marketing, for which there is not a harmonized legal definition in the European context yet. Generally, direct marketing "*consists of any advertising or marketing communication (whether trying to sell a product or to promote an organisation) that is directed to particular individuals or companies (…)*".[160] ICO has published its guidance on direct marketing, according to which, the term "*covers the promotion of aims and ideals as well as the sale of products and services*", meaning that it includes commercial and non-profit organisations, namely, *inter alia*, political

[158]The terms were based on ICO's guidance: Guidance on Political Campaigning. (2017). [ebook] ICO, p.2. Available at: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf [Accessed 19 Dec. 2017].

[159] Ico.org.uk. (2017). *Political campaigning practices*. [online] Available at: https://ico.org.uk/for-the-public/political-campaigning-practices/ [Accessed 22 Dec. 2017].

[160] Uk.practicallaw.thomsonreuters.com. (2017). [online] Available at: https://uk.practicallaw.thomsonreuters.com/4-385-3476?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [Accessed 22 Dec. 2017].

parties.[161] In their guidance on political campaigning, the definition of direct marketing is as follows: "*the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals*". The definition is further expanded on, as it is elaborated so that it also includes requests for funds or some other kind of support for political campaigns, such as a form of action or a vote for a particular political party or candidate. The definition further includes various forms of communication, such as online marketing, social networking or other developing channels of communication.[162] Despite the fact that the aforementioned definitions indeed render it possible to interpret Article 21 (2) GDPR as to be applicable in cases of political profiling as well, they still remain definitions applicable on a national level, not harmonized in the EU.

On January the 10th of 2017, the European Commission announced its draft proposal on the Regulation on Privacy and Electronic Communications (e-Privacy Regulation),[163] which contains some key provisions relating to the collection and use of personal data for direct marketing purposes. Article 4 (3) (f) of the draft text of e-Privacy Regulation defines the term 'direct marketing communications' as follows: "*any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc*." Recital 32 provides, among others, that the term also includes messages sent by political parties to natural persons in order for the first to be promoted.

Art.29WP published an Opinion on the proposed e-Privacy Regulation, according to which both the Article and Recital should be amended in order to include all advertisements sent, directed or presented to the end-user, so that all kinds of communication platforms are included, and it underlines that it should be ensured that 'behavioural advertisements' (based on the *profiles* of end-users) are included in the definition as well. It is also highlighted that apart from the advertising, marketing purposes should also be included in

[161] Direct Marketing. (2016). [ebook] Information Commissioner's Office, p.4. Available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf [Accessed 22 Dec. 2017].
[162] Guidance on Political Campaigning. (2017). [ebook] ICO, p.5. Available at: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf [Accessed 19 Dec. 2017].
[163] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003 (COD). 10 January 2017. Available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

the definition, so that individuals are protected from practices deployed by political parties that promote their political views or are related to political preferences, among others.[164]

In conclusion, individuals have the right to object as is formulated under Article 21 (1) GDPR, however this right could be overridden by political parties. It is debatable whether the right to object based on Article 21 (2) GDPR, which offers a higher level of protection, is currently granted to individuals who are subject to political profiling, as this depends on the "direct marketing" definition of each Member State's DPA. Nevertheless, this can change in the future, when the final form of the e-Privacy Regulation comes into force, especially if the aforementioned Opinion on the proposed draft is adopted by the final text.

2.5 Automated individual decision-making, including profiling

The next topic to be explored is whether individuals who are subject to political profiling can exercise the *right* not to be subject to automated decisions based solely on automated processing of their data. In order to reach a conclusion, an analysis of the rather complicated[165] Article 22 (1) GDPR has to be conducted.

Article 22 (1) GDPR provides that "*the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her".* What is noteworthy is the fact that "profiling" and "automated decision making" are two different procedures with different scopes: the first one, as already analysed, refers to the automated processing of personal data in order to develop analysed or predictive knowledge in the form of profiles that can be used as a basis for automated decision-making. The latter is perceived as the general ability to make decisions based on existing profiles, solely by automated technological means, meaning without the intervention of human involvement. Automated decision making essentially refers to the process of reaching a decision.[166] It should be noted that it is generally possible for automated decisions to be made with or without

[164] Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 4 April 2017, WP247, pp.20-21. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=44103.
[165] Veale, M. and Edwards, L. (2017). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. *Computer Law & Security Review*, [online] Forthcoming, p.2. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071679 [Accessed 30 Dec. 2017].
[166] Savin, A. (2014). Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks. *SSRN Electronic Journal*. [online] Available at: http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf?sequence=1 [Accessed 22 Dec. 2017].

profiling and for profiling to take place without necessarily resulting in automated decisions.[167]

The automated decision-making in profiling conducted for political campaigns purposes ought to be perceived as the decision relating to the kind and content of the personalised communication each profiling subject receives.

Before turning to the substantive content of Article 22 GDPR, a brief overview on the discussions regarding the nature of Article 22 (1) GDPR as a right or a prohibition will be presented here: Article 22 GDPR replicates Article 15 DPD, but with some changes. Therefore, the discussions around both Articles on the matter will be subsequently analysed. Article 15 (1) DPD reads as follows: "*Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.".* Although data protection regulations are in principle not prohibitive,[168] there are exceptions that set some prohibitive rules. Article 15 DPD has long been a "subject of confusion".[169] Gutwirth and de Hert, have supported that Article 15 DPD prohibits decision-making about an individual based exclusively on automated data processing.[170] On the other hand, Bygrave has extensively supported that Article 15 DPD does not prohibit a particular type of decision-making or profile application, rather it grants individuals a right to prevent them from being subjects to such decision-making when their personal data are processed.[171] According to Bygrave, data subjects should actively exercise this right of theirs, otherwise the targeted decision-making could take place in the absence of the right being exercised.[172] This point of view has been criticised by Gutwirth and de Hert, who believe that the legitimacy of a purely automated decision cannot depend on the inaction of the data subject that translates to implicit consent. They claim that the problematic point of this view is firstly the fact that subjects to automated decision-making

[167] Art.29WP, supra note 112 at p.8.
[168] Gutwirth, S. and de Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, p.282. Available at: https://link.springer.com/book/10.1007/978-1-4020-6914-7 [Accessed 22 Dec. 2017].
[169] Veale and Edwards, supra note 165 at p.5
[170] Gutwirth and de Hert, supra note 168 at p.283.
[171] Bygrave, supra note 124.
[172] However Bygrave supports the view that national legislators could implement Article 15 (1) DPD in terms of a prohibition on targeted decision-making.

are not consulted beforehand, and secondly that the concept of consent according to the Directive is this of a freely given and informed one. The view that Article 15 DPD sets a prohibition was also shared by the Belgian legislator when implementing the Directive.[173]
Regarding Article 22 (1) GDPR, Bygrave slightly changed his position, as he suggests that although it "invokes the language of a 'right'", it is mainly intended as a prohibition and not as a right that the data subject has to exercise.[174] The difference between the GDPR and the DPD, according to Bygrave, lies on the fact that national legislators implementing the Directive had the option to transpose it either as a right or a prohibition, which is not the case for the GDPR. Art.29WP also interprets the provision as a prohibition, clarifying the matter and putting an end to a long debate.[175] However, this view of Art.29WP has been criticised as "unauthorised law-making", since the language of the main provision from the DPD has remained essentially unchanged in the GDPR.[176] Treating the provision as a right or as a prohibition has an effect on the level of protection that is awarded to the data subjects, from a data protection perspective: a right, the exercise of which depends on the individual, is weaker and offers a lower level of protection than a prohibition does. Additionally, interpreting Article 22 (1) GDPR as a prohibitive rule is in accordance with the rationale of the Regulation which aims at empowering data subjects against the threats technological developments could bear, and when it comes to profiling practices in particular, aims at providing them with the ability to influence decision-making based on such practices.[177]

As already mentioned, Article 22 (1) GDPR refers to decisions based *solely* on automated processing, meaning that there is no human involvement in the decision process. Art.29WP states that human involvement should be seen as an important part of the decision making process, a human who has the authority and ability to change the decision for example. That way the controller cannot fabricate human involvement, by having for instance a human intervene in a rather unimportant part of the process, in order to avoid the applicability of the provision.[178]

[173] Gutwirth and De Hert, supra note 168 at p.283.
[174] Mendoza and Bygrave, supra note 17 at p.8.
[175] Art.29WP, supra note 112 at p.9.
[176] Veale and Edwards, supra note 165 at p.5.
[177] Mendoza and Bygrave, supra note 17 at p.5.
[178] Art.29WP, supra note 112 at p.10.

Article 22 (1) GDPR is only applicable in case the decision which is made and is based on an individual's profile, produces legal effects for that individual or significantly affects him or her. There is no definition of the "legal effect" in the GDPR and only two examples of "significant effects" are provided in Recital 71, namely the "*automatic refusal of an online credit application*" and the "*e-recruiting practices without human intervention*". A legal effect could be one that impacts the legal rights or status of an individual, such as the freedom to associate with others, the freedom to vote in an election or take legal action.[179] Even when no legal rights are affected, data subjects can still be protected under Article 22 (1) of the Regulation, when they are significantly affected. The significance should be equal to this of a legal effect, as the word *similar* suggests. A decision that "significantly affects" could be one that has the potential to influence the behaviour or choices of the individuals concerned.[180] It is rather difficult to precisely define these significant effects, as well as the type of profiling practices that they cover, but it has been claimed that they could include automated decisions, that are related to online targeted advertising, depending on the characteristics of each case, among which the intrusiveness of the profiling process, the way the advertisement is delivered etc.[181] It could be claimed that political profiling does indeed fall under the scope of this provision: the high degree of personalisation of the advertisements for political communication, which, according to research, bears a high degree of persuasiveness and influence,[182] could significantly affect individuals that receive them. Although a matter of interpretation, political profiling could produce legal effects, in the sense that individuals are not allowed to make fully informed choices and vote accordingly; receiving information is fundamental for people to participate in political life.[183] Detailed knowledge about the individuals gives the power to political parties to shape people's thinking and manipulate them into taking particular political decisions.[184] Based on the aforementioned, even if the decision-making process, that relates to the content of the targeted political ads, is not considered to have legal effects on individuals, it could be claimed that it significantly affects them anyway, as it does have the potential to influence

[179] Ibid.
[180] Ibid.
[181] Art.29WP, supra note 112 at p.11.
[182] Helberger, N. (2016). Policy Implications From Algorithmic Profiling and the Changing Relationship Between Newsreaders and the Media. *Javnost - The Public*, [online] 23(2), pp.193, 195 and 197. Available at: http://www.tandfonline.com/doi/full/10.1080/13183222.2016.1162989 [Accessed 22 Dec. 2017].
[183] Eskens, S., Helberger, N. and Moeller, J. (2017). Challenged by news personalisation: five perspectives on the right to receive information. *Journal of Media Law*, 9(2), p.264.
[184] Helberger, supra note 182 at pp.192-194.

their behaviour and choices.[185] Judging on the large amounts of data collected and used for political profiling, the extremely high degree of personalisation and the intrusiveness that profiling for such reasons seems to have, it would be appropriate to classify automated decisions based on political profiling as a form of prohibited decision-making under Article 22 (1) GDPR. Therefore, automated decision-making based on political profiling, including (political) profiling,[186] could be carried out only if one of the exceptions provided by Article 22 (2) GDPR applies.[187] It seems rather non-realistic for political parties to be able to base their profiling practices and automated decision-making on any of the grounds for exceptions, other than national legislation (Article 22 (2) (b) GDPR). It remains to be seen in practice how political profiling practices could be implemented in accordance with the Regulation, provided that they become more transparent. Indeed, it has so far been extensively discussed by legal scholars that these practices are surrounded by secrecy and opacity, [188] and the practical implementation of data protection laws that supposedly empower data subjects through measures that promote transparency, has been criticised as rather complicated.[189] For these reasons, it is debatable whether we can be "optimistic about the effectiveness of the obligations and rights in terms of the transparency they can provide"[190] and consequently the effectiveness of the Regulation, at least when it comes to the provisions that regulate profiling or political profiling for that matter.

[185] Gutwirth and De Hert, supra note 168 at p.291.

[186] Profiling and automated decision-making have different scopes and may partially overlap. Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However they are not necessarily separate activities either. The GDPR addresses three potential ways in which the concept of profiling can be used: as *general profiling* (Article 4 (4) GDPR); as *decision-making based on profiling;* and as *solely automated decision-making, including profiling* (Article 22 GDPR).

[187] Article 22 (2) states that Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

[188] Gutwirth and De Hert, supra note 168 at pp.289 and 291. See also: Bosco, Creemers, Ferraris, Guagnin and Koops, supra note 117 at p.13. See also: Art.29WP, supra note 112 at p.10.

[189] Bosco F., Creemers N., Ferraris V., Guagnin D., Koops BJ. (2015) Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities, p.13. In: Gutwirth S., Leenes R., de Hert P. (eds) Reforming European Data Protection Law. Law, Governance and Technology Series, vol 20. Springer, Dordrecht

[190] Hildebrandt, M. (2008). Profiling and the Identity of the European Citizen. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, p.314. Available at: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_15 [Accessed 29 Dec. 2017].

2.6 Special categories of personal data and political profiling

Data revealing political opinions is explicitly defined as a "special" form of personal data in the GDPR. Article 9 (1) of the Regulation[191] prohibits the processing of personal data revealing, among others, political opinions. The categories of data characterised as special in the GDPR reflect those mentioned in the Council of Europe Convention 108 and are also rooted on the principle of non-discrimination based on political opinion, as is safeguarded by Article 21 of the Charter of Fundamental Rights of the European Union.[192] Earlier guidance provided by Art.29WP on the Directive's special categories of data, states that the rationale behind the difference in regulation stems from the severe and irreversible consequences for the individuals' fundamental rights that the misuse of this data could cause.[193] Therefore the prohibition of the processing of such data is justified by the fact that this would threaten fundamental rights and freedoms, as is also enhanced by Recital 51.[194] Profiling done within the context of political campaigns directly aims, by definition, at unveiling political preferences and opinions of the profiling subjects. According to Art.29WP, special category of data can be derived or inferred from profiling activities. Profiling can create special categories of data by inference of data which are not special categories on their own, but become so when combined with other data.[195]

Article 9 of the GDPR applies to both profiling and automated decision making. Despite the fact that, according to the aforementioned, political profiling is a prohibited form of processing of personal data, this prohibition is not absolute; Article 9 (2) GDPR provides the grounds for derogation from the main prohibitive rule. According to Article 9 (2) (d) GDPR, processing that is carried out from a foundation, association or any other non-profit body

[191] Article 9 (1) GDPR reads as follows: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

[192] Bennett, supra note 22 at p.266.

[193] Article 29 Data Protection Working Party. Advice paper on special categories of data ("sensitive data"). 20 April 2011. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. For the practical complications of this interpretation look at Goodman, B. and Flaxman, S. (2016). *European Union regulations on algorithmic decision-making and a "right to explanation"*. 3rd ed. [pdf] New York: University of Oxford, p.4. Available at: https://arxiv.org/pdf/1606.08813.pdf [Accessed 18 Dec. 2017].

[194] Recital 51 of the GDPR reads as follows: "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. (…)".

[195] Art.29WP, supra note 112 at p.22.

with a political aim in the course of its legitimate activities is allowed, as far as appropriate safeguards are provided,[196] on the condition that the processing relates solely to members of the body (or former members thereof) or to people who have regular contact with it.[197] Recital 51 justifies derogations from the general prohibition of the processing of special data from foundations or organisations whose purpose is to permit the exercise of fundamental freedoms. Political parties are considered non-profit bodies.[198] Accordingly, profiling that enables the revealing of political preferences and opinions of data subjects is allowed, when it relates to members or former members of the political parties that deploy the profiling methods or when it concerns individuals that have *regular contact* with them. The latter seems to be rather problematic to interpret, as the question how this "regular contact" is measured and with which means, arises.

Automated decision making, including profiling, that is based on special categories of data is only allowed, according to Article 22 (4) GDPR, under the exceptions provided by Article 9 (2) (a) and 9 (2) (g) GDPR, explicit consent of the data subject and processing necessary for reasons of public interest respectively. Assuming that it is highly unlikely that political parties could base their profiling practices and automated decision-making (relating to the personalised communication that potential voters receive) on consent as described below, the public interest as a ground for exception should be examined. Indeed, Recital 56 allows for exceptions from the main prohibitive rule in the name of the operation of the democratic system of Member States, which requires for political parties to accumulate data on people's political opinions during the course of electoral activities for reasons of public interest, provided that appropriate safeguards are established. According to this Recital, not

[196] Recital 71 of the GDPR highlights that these safeguards 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.

[197] Article 9 (2) (d) GDPR reads as follows: "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;".

[198] Breen, O. (2008). EU Regulation of Charitable Organizations: The Politics of Legally Enabling Civil Society. *The International Journal of Not-for-Profit Law*, [online] 10(3). Available at: http://www.icnl.org/research/journal/vol10iss3/special_3.htm [Accessed 31 Dec. 2017]. See also Casey, J. (2016). Comparing Nonprofit Sectors Around the World: What Do We Know and How Do We Know It?. *Journal of Nonprofit Education and Leadership*, [online] 6(3), pp.192, 210. Available at: http://js.sagamorepub.com/jnel/article/view/7583 [Accessed 31 Dec. 2017]. See also Neely, S. (2003). Non-Profits, Not-for-Profits, and Charities: What's the Difference?. *The Scrivener*, [online] 12(3), p.11. Available at: https://www.notaries.bc.ca/resources/scrivener/fall2003/12_3_5.pdf [Accessed 31 Dec. 2017].

only profiling, but also decision-making that is based on individuals' special data could take place by political parties for reasons of public interest.

Examining the grounds for exception provided by Articles 9 (2) (a) and (e) GDPR, the following should be noted: individuals can be subject to political profiling (and automated decision-making) in case they give their *explicit consent* and in any case profiles can be created by processing data that was *manifestly made public by the data subject*. Nowadays, it has become really hard for individuals to control where they leave their digital footprint and assess the implications this might have on their privacy-related rights, as well as essentially comprehend the prospective use or application each of their data points can have and consent to it, especially when combined with other data points made public by them. That means that it is either impossible for political parties to base their processing activities on individuals' consent, or that individuals' will give their consent, without being fully aware of which of their data is used for these activities. Quoting Gutwirth and de Hert, *"humans have become detectable, (re)traceable and correlatable far beyond their control"*.[199] Consequently, when individuals are unaware of every processing activity regarding their data or at least the extent thereof, it is practically impossible to evaluate the legitimacy of such processing and eventually file a legal complaint when necessary.[200] For that reason, it seems that, ultimately, the protection that the GDPR aspired to provide individuals with, unfortunately does not cover entirely thousands of individuals who are subject to political profiling.

2.7 Conclusion

Political profiling is a form of profiling regulated by the GDPR. Individuals have the right to be informed about the fact that they are subjects to political profiling, the logic involved in any automatic processing of their personal data and lastly about the consequences such practices might have on them. They are also entitled to receive the personal data concerning them or data that has been provided to a controller, in a structured, comprehensive, machine-readable and interoperable format and transmit it to another controller,[201] in order to strengthen their control over their data. Individuals can exercise the right to object based on Article 21 (1) GDPR, however some opportunities for the controller

[199] Gutwirth and De Hert, supra note 168 at p.291.
[200] van der Sloot, supra note 48 at p.430.
[201] Recital 68 of the GDPR.

to override the provision become apparent. The exercise of the right based on Article 21 (2) GDPR, currently depends on each Member State's definition of "direct marketing", however, a harmonized definition of the term in the EU context could secure this right for political profiling subjects in the future. The right not to be subject to automated decision making, based on Article 22 (1) GDPR, which is linked to profiling, is attributed to individuals who are subject to political profiling, however the practical implementation of the provision could eventually be complicated. Additionally political parties could base their automated decision-making on the exception provided by Articles 22 (2) and 9 (2) (g) GDPR, this of processing necessary for reasons of public interest. Finally, although political profiling reveals by definition political opinions of data subjects, which constitute according to Article 9 (1) GDPR a special category of personal data, there are many exceptions of the main prohibitive rule of the processing of such data, which ultimately render such profiling permissible, minimizing at the same time the scope of protection for individuals.

Chapter 3: Is regulation enough? Where to focus next

This chapter is looking into means that could reinforce individuals' protection against political profiling practices, touches upon the discussions around the prohibition of profiling, weighs in on the idea of the prohibition of political profiling and explores alternatives to it. It emphasises the importance of future research and proceeds to explore the first steps that have been taken towards this direction, that are not only based on the principle of transparency, but also contribute to its actual realisation.

3.1 A call for further research

After having explored the profiling practices deployed by political parties, the sources, types and amounts of data collected for the realisation of such practices, the application and use of the profiles generated, the threats that these practices bear for the rights of the data subjects, as well as the implications they could have on society as a whole, the focus of this thesis shifted on the regulation of political profiling from the perspective of data protection law. The extent to which political profiling is regulated, both in the US and in the EU, was subsequently explored, with greater emphasis on its regulation under the upcoming GDPR. The rights and therefore the protection granted to individuals who are subject to political profiling were investigated, with the conclusion being that US citizens are left completely unprotected, when European citizens are awarded some rights that could be used as a defence to political profiling, which is not prohibited in its entirety under the GDPR. However they are either weak or complicated in practice. It was consequently deemed necessary to explore whether these rights could be empowered and if so with which means. The first issue this study will consider for this reason is whether profiling conducted for political communication should be entirely prohibited.

Before an answer can be provided to this question, the debate regarding the prohibition of profiling in general will be touched upon. Legal scholars have extensively discussed the threats profiling practices can pose to citizens' privacy, data protection and other fundamental rights as well as the rule of law.[202] For this reason the question whether profiling should be prohibited has arisen. However, posing this question seems to be problematic in the first place, as we cannot condemn profiling in general, but rather have to

[202] Hildebrandt, supra note 190 at pp.309-311.

explore the issue of its prohibition within certain contexts.[203] Koops has suggested that only particular types of profiling can affect people's lives and their fundamental rights, and therefore these are the ones people should worry about.[204] Precisely indicating the type of profiling is crucial when exploring the issue of its prohibition. What is also of particular importance for the matter is the type of (negative) impact it can have on individuals' lives and rights. These negative impacts should be calculated and supported by extensive research,[205] as simply prohibiting some forms of profiling based on theory, in abstract, and not on scientific data, could be faced with disbelief or, even worse, resistance from the profilers. Another critical point of relevance is the use and application of the generated profiles; the extent to which profiling practices carry the risk of manipulating individuals' behaviour should be investigated, in addition to whether such practices can lead to major shifts in power between the profilers and the profiled.[206]

As highlighted in the previous chapters, political profiling practices nowadays are rather intrusive, bear risks of manipulation of individuals and can, if not already do, cause a shift in power between political parties and voters; it has been explained how political parties use the high degree of personalisation of political ads enabled by profiling in order to benefit themselves.[207] Profiling for political communication is therefore an issue, the risks of which should be addressed. Is the prohibition thereof, however, an effective and most importantly realistic way to tackle these risks?

For some types of profiling, prohibition has been proposed as the best way to minimize the effects they can have on individuals; Borgesius has suggested that lawmakers should consider banning *personal data collection for behavioral targeting and similar purposes on public service media*.[208] Helberger also agrees with this point of view.[209] Proposals for the prohibition of profiling that could have the effect of discrimination on the basis of special

[203] Borgesius, supra note 143 at p.366.
[204] Koops, B. (2008). Some Reflections on Profiling, Power Shifts, and Protection Paradigms. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, p.328. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350584 [Accessed 1 Jan. 2018].
[205] Ibid. at p.337.
[206] Koops, supra note 2014 at p.333.
[207] Koops, see supra note 204 at p.333.
[208] Borgesius, supra note 143 at p.388.
[209] Helberger, supra note 71 at p.196.

categories of data have also been made.[210] Outside Europe, a number of American States have enacted legislation to prohibit "racial profiling".[211] However, agreeing on prohibitions can be very challenging for the lawmakers. Additionally, suggesting the prohibition of political profiling at this point seems rather unrealistic and therefore pointless: the proposal for the *prohibition of profiling that is based on or generates special categories of data* has already been rejected by the final text of the GDPR.[212] During the *travaux préparatoires* of the GDPR the challenges and effects that would accompany political profiling had likely not become fully apparent, so imposing full prohibition on political profiling, which in itself was almost not at all discussed, would possibly seem to be too blunt of an instrument. For the US, such proposal seems to be utopian, as the only protection individuals have when it comes to their data protection, stems from the system of self-regulation.[213] Since the solution of prohibition of political profiling does not seem to be viable or achievable, alternatives that would empower profiling subjects should be examined.

The author of this thesis agrees with many legal scholars and academics that have written on the topic of profiling and call for further research. Extensive research is deemed still imperative today, in order to illuminate every possible impact this area of practice could have on individuals' lives and rights. This is even more true when it comes to political profiling that is typically surrounded by secrecy and opacity.[214] Its implications have not yet been made fully apparent, neither are supported by convincing qualitative and quantitative data to date. Koops suggests that further research should shed light on the consequences of different types of profiling on people's lives.[215] Borgesius understands that future research on profiling is the necessary prerequisite of a prohibition thereof, in order for the latter to be neither over nor under inclusive.[216] Helberger emphasises the importance of cross-disciplinary research, as law and technology are increasingly intertwined.[217] As more

[210] Douwe, K. (2012). Comments on Selected Topics in the Draft EU Data Protection Regulation. [online]. p.19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2150145 [Accessed 1 Jan. 2018].
[211] *H.R.3618 - 112th Congress (2011-2012): End Racial Profiling Act of 2011*. [online] Available at: https://www.congress.gov/bill/112th-congress/house-bill/3618?resultIndex=5 [Accessed 1 Jan. 2018].
[212] Article 20(3) of the LIBE Compromise, proposal for a Data Protection Regulation (2013). In his draft report, Rapporteur Albrecht had proposed to prohibit all profiling that includes or generates special categories of data (Draft Albrecht report, amendment 162, article 20(3)). Available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.
[213] Look at Chapter 1.4 of this thesis.
[214] Bosco, Creemers, Ferraris, Guagnin and Koops, supra note 117 at p.13.
[215] Koops, supra note 204 at p.329.
[216] Borgesius, supra note 143 at p.422.
[217] Helberger, supra note 71 at p.199.

and more voters encounter or will encounter, in the near future, political micro-targeting and be subject to profiling practices, further research would facilitate them understand this transition and what it actually means for them.[218] There are therefore a number of questions that could be posed and hopefully answered in this direction: to what extent is profiling used for political communication in the European grounds? ICO's currently ongoing investigation on the topic is a welcome first step towards answering this question. Is political micro-targeting indeed more persuasive than other forms of political communication? Are profiled voters more extreme in their opinions and is this connected in any way to the method of political profiling? Are there any groups of people that are completely left out from such means of political communication? Are voters aware that they are being profiled and if so, has this lead to any changes in their (voting) behaviour?[219] Are individuals aware of the rights they are awarded by law against political profiling? Answering those questions would indicate which next steps should society and the law take, and would likely reinforce legal scholars' arguments related to the dangers for the individuals' rights that come with these practices.

3.2 Transparency through technological applications: ongoing developments

This section of the thesis explores the principle of transparency and examines technological applications that aim at achieving the realisation of this principle. In data protection law, the legislator did not, in principle, choose the prohibition of data collection, its analysis and application to individuals (profiling). [220] These activities however are submitted to transparency rules and should consequently be carried out in accordance with them. The value of transparency of profiling methods in general has been emphasised by many. Gutwirth and de Hert have argued that there is no need for prohibitive measures on profiling as long as transparency is guaranteed. [221] They believe in transparency through regulation that provides citizens with tools of control, which subsequently compel the powerful parties of the equation to implement good practices, limiting at the same time their opportunities for

[218] Barocas, supra note 58 at p.34.
[219] Barocas, supra note 58 at p.34.
[220] This statement refers to EU data protection law, since as has already been emphasised, data protection laws in the US are practically non-existent. Also look at Gutwirth and de Hert, supra note 168 at p.282.
[221] Gutwirth and de Hert, supra note 168 at p.290.

abuse of power.[222] Transparency should be particularly focused on the decision-making and its interrelation with special categories of data. That way data subjects are empowered through the ability to check, assess and possibly seek remedies for unjust judgements based on these data.[223] Lack of transparency related to certain types of profiling, such as the political one, that have the potential to undermine the legal rights and freedoms of citizens, can "cripple" individuals and fundamentally change the society they live in.[224] Although transparency is dictated by data protection law, it is only through technology and its applications that it can be achieved. In practice, this principle is translated into tools that ensure the visibility of profiling practices and enforce individuals' controllability and profilers' accountability.

For this reason, some illustrations of how the principle of transparency related to political profiling could potentially be implemented, are presented next. Online tools that have the potential to allow individuals to become aware of the fact that they are being tracked and targeted with personalised political messages online, have started emerging during the past year. The majority of these tools were created by civil society, with the cooperation of researchers, journalists and academics. One of the first projects that intended to bring transparency to political advertising online was initiated back in 2012 by Barocas, who introduced the "Soap Box" project.[225] Acknowledging the fact that political campaigns use an ever-increasing number of online data points, in order to track and target voters with tailored messages for political communication, the project aimed at transforming these opaque practices into transparent by reinstating political debates in a more public forum. For this reason the project proposed to track, record and pool political advertising messages, so that political profiling practices become subject to public scrutiny. The project also intended to precisely answer the question of what kinds of data are used for such purposes and additionally develop mechanisms that would automatically identify and record cases of targeted political advertising. The exposure that Soap Box would bring to these practices would, among others, result in political parties being generally more hesitant to

[222] Gutwirth, S. and de Hert, P. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: E. Claes, S. Gutwirth and P. de Hert, ed., *Privacy and the criminal law*. Antwerp/ Oxford: Intersentia.

[223] Leenes, R. (2009). Reply by Ronald Leenes (TILT): Addressing the Obscurity of Data Clouds. TILT Law & Technology Working Paper No. 012/2009; Tilburg University Legal Studies Working Paper No. 008/2009. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1393193 [Accessed 2 Jan. 2018].

[224] Koops, supra note 204 at p.335.

[225] Solon.barocas.org. (n.d.). *Soap Box | Solon Barocas*. [online] Available at: http://solon.barocas.org/?page_id=38 [Accessed 2 Jan. 2018].

adopt extreme positions in targeted messages than they would in more public forums. It would additionally discourage parties to collect and process information about individuals without them being aware and prevent them from excluding some individuals from their political communication completely. However, the practical challenges that this project was faced with were that data regarding the criteria, which determined what messages voters received, were limited and political parties were not willing to cooperate in order to provide further information on the matter. The solution of the project being based on voluntary submissions of automated online political ads was rejected, as it would likely result in biased and incomplete results and could even lead to intensifying the chilling effect these practices already have.[226] The project was eventually absorbed by other, ongoing, research initiatives.[227]

The Soap Box project and its evolution illustrate the difficulties that arise during the research in the area of profiling in general, and particularly in this of political profiling. It becomes evident that the initiative for research of one researcher or one institution alone is not enough in itself and requires the cooperation and active participation of political parties and citizens. However, it seems highly unlikely that political parties would ever contribute to a research that could result in exposing their practices, which are associated with a negative impact on individuals' rights and freedoms. During 2017, in light of the barrage of revelations related to the use of profiling practices by political parties worldwide, a number of initiatives aiming at enhancing digital transparency appeared.

The New York based non-profit organisation ProPublica aims at increasing *transparency and accountability of elections around the world,* by monitoring political advertising on Facebook.[228] In September 2017 ProPublica launched "PAC", brief for Political Ad Collector, a crowdsourcing tool that gathers political ads from Facebook, which is the biggest online platform for political discourse. This tool is not dependent on the involvement of any political parties; users of the social network platform are asked to download and add the software on their web browser and subsequently monitor the advertisements during election periods

[226] Barocas, supra note 58 at p.34.
[227] The project has been absorbed into the Princeton Web Transparency & Accountability Project that studies privacy, security and ethics of consumer data usage. Available at Webtap.princeton.edu. (2018). *Princeton WebTAP – Web Transparency & Accountability Project @ Princeton*. [online] Available at: https://webtap.princeton.edu/ [Accessed 2 Jan. 2018].
[228] Angwin, J. and Larson, J. (2017). *Help Us Monitor Political Ads Online — ProPublica*. [online] ProPublica. Available at: https://www.propublica.org/article/help-us-monitor-political-ads-online [Accessed 2 Jan. 2018].

themselves. It has already been tested in September during the German parliamentary elections that attracted international interest due to the rise of an anti-immigration political party. PAC identifies, with the help of an algorithm, which of the advertisements on the users' Facebook feed are political and allows users to have access to political ads that were not originally aimed at their demographic group and were not intended to be presented to them. All the collected political ads are added to a public database rendering them visible to anyone interested. The PAC tool is still new and no official results have been published in its database to date.

Another similar initiative is the "Who Targets Me" citizen led non-partisan project, which is aiming at monitoring the use of dark ads[229] during elections worldwide.[230] With the help of a browser extension, Who Targets Me can inform Facebook users which political campaigns use dark ads and micro-targeting to influence their voting behaviour. The project, which was initiated due to the global deficit of research in the area of profiling practices for political communication purposes, makes use of anonymous data to further investigate into the extent of such targeting.

"Project DATA, Digital Ad Tracking and Analysis", that is funded by a consortium of research organisations, is collecting campaign data in order to analyse how political parties, organisations and candidates are disseminating targeted digital messages to potential voters.[231] It uses data collected either by a web browser extension or donated by citizens, who are willing to contribute to the research. Project DATA aims, too, at improving transparency around political profiling methods and ultimately at reinforcing democratic practices.

Despite the fact that the aforementioned initiatives constitute a good example of how technology can be used at the services of the transparency principle, they all remain projects introduced by civil society. Most projects are still in their infancy and results from their research are yet to be officially published. Participants and users of these tools may not compose a representative portion of the population, which bares the risk of research

[229] The term "dark ads" or "dark posts" is distinguished from a normal advert or Facebook post by the fact that it is never seen by anyone except the intended recipient.
[230] Who Targets Me?. (2017). *About us - Who Targets Me?*. [online] Available at: https://whotargets.me/en/about/ [Accessed 2 Jan. 2018].
[231] Eyeonelections.com. (2016). *Project DATA | Digital Ad Tracking and Analysis*. [online] Available at: http://www.eyeonelections.com/ [Accessed 2 Jan. 2018].

generating biased results. Nevertheless, such initiatives are a welcome starting point. The creation of user-generated political ads databases is probably one of the best ways to engage citizens, raise awareness towards the issue of political profiling and compel political parties to employ good practices. Similar initiatives and technological tools would most likely be successful in the future, as, with each election cycle, the debate around political profiling is bound to grow bigger, more and more voters would become aware of the issue and get further involved. Accordingly, these tools present also an opportunity to restore the balance of power between political parties and voters, allowing individuals to surpass the limits that personalized messages put to political communication.

Similar transparency-enhancing tools and applications could also be imposed by national legislators that would require political parties to launch them as a mandatory part of their online campaigns. For the latter to be achieved however, a form of social pressure has to be created first, ideally supported by qualitative and quantitative data that would be the result of prior research, as has already been suggested. Civil society-initiated research could provide such data. Given the fact that political profiling seriously interferes with the rights and freedoms of individuals, such pressure does not seem to be entirely unachievable.[232] In case Member States enact legislation that would demand political parties to develop and employ such tools, compliance with the GDPR, which asks for a high degree of transparency when it comes to data collection, automated- decision making and profiling practices, would be achieved.[233] For the US, where data protection laws are practically non-existent and the system of self-regulation is dominant, these tools and the results from the research they initiate could be used as the engine for pressure towards the enactment of data protection legislation.

3.3 Conclusion

A binary deduction from the previous chapter is what led to the third and last chapter of this thesis: on the one hand the regulation of political profiling comes with exceptions that allow millions of individuals to be subject to such practices. On the other hand the practical implementation of several provisions regulating profiling seems rather complicated. It was therefore deemed appropriate to explore, not only whether blunter instruments of regulation are necessary, but also ways that would facilitate the implementation of the law. For this

[232] Koops, supra note 204 at p.336.
[233] Look at Recitals 39, 58, 59, 60 and Articles 12, 13, 14 GDPR.

reason the first part of this chapter explored the idea of the prohibition of political profiling in its entirety, which was ultimately rejected; not only would such prohibition would be too extreme of a measure, due to the so far absence of any qualitative and quantitative data that would imperatively dictate it, but would also constitute a rather unrealistic proposal. Further research is viewed as the appropriate prerequisite of a measure such as prohibition. This chapter suggests a series of questions that could be explored in order to illuminate the impact political profiling practices can have on individuals, their rights and even society as a whole. Relating to the practical implementation of the provisions that regulate profiling, the principle of transparency could be proved to be the means that would empower citizens who are subject to political profiling practices. An overview of examples of transparency-enhancing tools and technological developments, related to political profiling, that have only recently started to come to life was presented. Further development of these tools and the results that would be generated from the research that they initiate could additionally be used as a form of social pressure and as the stepping stone for the enactment of data protection legislation in the US.

Conclusion

Profiling practices for political communication are increasingly becoming the new norm in the United States; big data analytics companies do not only openly advertise their involvement in the federal and state elections, they also take pride in the elections' outcome, acknowledging the fact that their practices are so powerful that they can even designate the next US President.[234] In the latest years it became apparent that these practices are expanding into the EU grounds, therefore an investigation of their regulation both in the US and in the EU, from a data protection perspective, was deemed academically interesting.

In the United States, sources of data that are used for political communication include information ranging from real estate records and vehicle registration to credit card records and magazine subscriptions. Additionally, individuals' digital footprints, like information about the content "shared" or "liked" on social media, online activities and behavior are closely monitored and analysed in order to subsequently group potential voters into profiles, in a manner that allows for accurate predictions regarding their voting behaviour. The latter refers to the method known to the US as "micro-targeting", which enables political parties to deliver personalised messages to potential voters by applying predictive modelling techniques that achieve remarkably efficient means of communication.

Micro-targeting and profiling practices have been associated with a number of concerns raised by academics and civil society in relation to the citizens' information and political privacy rights. Such practices, due to their degree of personalisation, are likely fragmenting political communication; it is possible that individuals receive communication that addresses divisive issues that would likely not be addressed in a public debate, and in some cases people can be completely excluded from receiving any political communication at all, leading to a form of "political redlining". Public political debates could be hindered and the entire democratic procedure of elections could be jeopardised. These methods are also surrounded by a high degree of opacity and the communication that they enable has been claimed to be highly persuasive, even manipulative.

In spite of the fact that such practices are greatly intrusive, political parties and entities in the US generally enjoy vast liberty when processing (potential) voters' data for political

[234] Look at supra note 1.

communication purposes, mainly because their restriction would be opposed to their freedom to communicate their messages to citizens, which is protected under the First Amendment. Additionally, there are no comprehensive data protection laws on a federal level and at the same time, privacy regulations on a state level offer inadequate protection to citizens who are subject to political profiling. For this reason, there is a tendency towards self-regulation, which is also being supported by the FTC. However this self-regulatory system is not enforceable by law, meaning that until the US Congress enacts legislation that would address these issues, millions of Americans are defenseless against political profiling.

In the EU, the processing of personal data by political parties, as well as marketing and big data analytics companies that work for these parties, is currently regulated by the Data Protection Directive which is soon going to be succeeded by the General Data Protection Regulation. The latter has been the major focus of this thesis, as it explicitly regulates profiling. Political profiling, term which refers to profiling conducted by campaigners in the course of electoral campaigns for political communication purposes, is a form of profiling that is regulated under the GDPR.

The focus of this thesis fell on two provisions of the GDPR, Article 21, the right to object, and Article 22, automated individual decision-making, including profiling. It was particularly examined whether individuals who are subject to political profiling are protected under these two provisions of the Regulation. Individuals have the right to object, on grounds relating to their particular situation, to the processing of their personal data, where the basis for that processing is either public interest or legitimate interests of the controller (Article 21 (1) GDPR). Campaigners could however demonstrate compelling legitimate grounds for such processing, which they have to prove, in order to deny the ceasing of processing. Article 21 (2) GDPR, which refers to the right to object to processing of personal data for the purposes of direct marketing, is an absolute right, that provides higher safeguards for the data subjects. Nevertheless, due to the lack of a harmonised definition of the term *direct marketing,* which could potentially cover the profiling methods that are used by campaigners for political communication purposes, this right is likely not granted to political profiling subjects yet.

Regarding Article 22 GDPR, the following are noteworthy: despite the wording of the provision's first paragraph, this Article is perceived as a prohibition and not as a right per se. This affects the level of protection that this provision grants to individuals. Article 22 (1) GDPR is only applicable in case the solely automated decision that is being made and which is based on an individual's profile produces legal effects or significantly affects this particular individual. Recalling the concerns that are associated with the profiling practices and the threats they possibly pose to the individuals' privacy and data protection-related rights, it could be claimed that automated decisions based on political profiling are classified as a prohibited form of decision-making under the GDPR. Article 22 (2) GDPR provides the legal grounds for exceptions of this prohibition. It remains to be seen how this provision will be practically implemented once the GDPR becomes effective, considering that profiling practices are very much opaque to date.[235]

Article 9 GDPR applies to both profiling and automated decision making. Under the first paragraph of this provision political profiling is considered to be a prohibited form of processing of personal data. However the second paragraph provides the grounds for exception of the main prohibition, which ultimately render such profiling conducted by political parties permissible.

Finally, the GDPR grants individuals the right to be informed about the fact that they are subject to political profiling, the logic involved in any automatic processing of their personal data, as well as the consequences such practices might have on them.[236] They are also entitled to receive personal data concerning them or data that have been provided to a controller, in order to have a higher control over their data.[237] The scope of this thesis doesn't allow for further expansion on these particular rights, each one of which merits particular academic consideration.

Throughout the thesis it became apparent that the GDPR provides a more comprehensive framework of protection and offers better legal safeguards for the data subjects than the self-regulatory US system does. As emphasised in the introduction of this thesis, the two majorly different legal and political systems do not allow for an explicit comparison, hence

[235] Art.29WP, supra note 112 at p.13; controllers' transparency obligations are emphasised in light of the potential risks that profiling caught by Article 22 GDPR poses to the rights of data subjects.
[236] Look at Articles 13 (2) (f) and 14 (2) (g) GDPR, as well as Recitals 39, 58, 60.
[237] Look at Article 15 GDPR; for solely automated decision-making look at Article 15 (1) (h) GDPR.

the research was restricted to the description and analysis of the two regulatory frameworks and the extent to which they regulate the issue of profiling for political communication purposes. Despite the fact that the topic is indeed regulated under the GDPR, the extent to which profiling subjects are actually safeguarded against this type of profiling is not entirely clear yet. It is expected that this is an area which will be illuminated once the GDPR comes into force. At that time most practical implications of the implementation of the Regulation, which are currently discussed on a theoretical level, are also likely to become apparent.

When the current regulation does not seem to provide the maximum level of protection to profiling subjects, the next step is to explore whether stricter legal measures should be taken in order to achieve that. For that reason this thesis reviewed discussions around the idea of the prohibition of profiling, and applied them to the concept of political profiling. This measure is ultimately deemed to be not only rather extreme, but premature as well, both in the US and in the EU, due to the lack of research that could potentially generate data which would excuse such a blunt measure. The last part of the thesis examines how the principle of transparency, which is of particular importance when it comes to profiling practices, could be used as the initiator of technological developments and applications, which would ultimately reinforce this principle itself. The fact that there are already a number of such applications, although in their infancy, constitutes a very optimistic sign that in the future, political profiling practices could potentially be elucidated and consequently their regulation could respectively become more targeted and effective.

List of references

Books and Chapters of books

Bosco, F., Creemers, N., Ferraris, V., Guagnin, D. and Koops, B. (2015). Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. In: S. Gutwirth, R. Leenes and P. de Hert, ed., *Reforming European Data Protection Law*. [online] Dodrecht: Springer, pp.3-33. Available at: https://link.springer.com/chapter/10.1007/978-94-017-9385-8_1.

Gutwirth, S. and de Hert, P. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: E. Claes, S. Gutwirth and P. de Hert, ed., *Privacy and the criminal law*. Antwerp/ Oxford: Intersentia, pp.61-104.

Gutwirth, S. and De Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.271-302. Available at: https://link.springer.com/book/10.1007/978-1-4020-6914-7.

Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge?. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.17-45. Available at: https://link.springer.com/chapter/10.1007/978-1-4020-6914-7_2.

Hildebrandt, M. (2008). Profiling and the Identity of the European Citizen. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.303-343. Available at: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_15.

Hildebrandt, M. (2009). Profiling and AmI. In: K. Rannenberg, D. Royer and A. Deuker, ed., *The Future of Identity in the Information Society*. [online] Berlin: Springer, pp.273-310. Available at: https://link.springer.com/chapter/10.1007/978-3-642-01820-6_7.

Hildebrandt, M. (2017). Who is Profiling Who? Invisible Visibility. In: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne and S. Nouwt, ed., *Reinventing Data Protection?*. [online] Dodrecht: Springer, pp.239-252. Available at: https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_14.

Hillygus, D. and Shields, T. (2009). *The Persuadable Voter Wedge Issues in Presidential Campaigns*. Princeton: Princeton University Press.

Howard, P.N. (2005). *New Media Campaigns and the Managed Citizen*. Cambridge University Press.

Koops, B. (2008). Some Reflections on Profiling, Power Shifts, and Protection Paradigms. In: M. Hildebrandt and S. Gutwirth, ed., *Profiling the European Citizen*. [online] Dordrecht: Springer, pp.326-337. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350584 .

Mendoza, I. and Bygrave, L. (2017). The Right Not to Be Subject to Automated Decisions Based on Profiling. In: T. Synodinou, P. Jougleux, C. Markou and T. Prastitou, ed., *EU Internet Law: Regulation and Enforcement*. [online] Springer, Forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855.

Savin, A. (2015). Profiling in the Present and New EU Data Protection Frameworks. In: P. Nielsen, P. Schmidt and K. Dyppel Weber, ed., *Erhvervsretlige emne*. Juridisk Institut CBS.

Skouma, G. and Léonard, L. (2015). On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. In: S. Gutwirth, R. Leenes and P. de Hert, ed., *Reforming European Data Protection Law*. [online] Dordrecht: Springer, pp.35-60. Available at: https://link.springer.com/chapter/10.1007%2F978-94-017-9385-8_2.

van der Sloot, B. (2016). Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: S. Gutwirth, R. Leenes and P. De Hert, ed., *Data Protection on the Move*. [online] Dodrecht: Springer, pp.411-436. Available at: https://link.springer.com/book/10.1007/978-94-017-7376-8#toc.

Case-law

Lingens v Austria no 9815/82, 8 July *1986*, *Series A no 103*, (*1986*) 8 EHRR 40, ECtHR.

ebooks and PDFs

Direct Marketing. (2016). [ebook] Information Commissioner's Office. Available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf.

European Data Protection Regulation: Information Sheet. (2016). [ebook] Privacy Europe. Available at: https://www.privacy-europe.com/blog/wp-content/uploads/2016/03/European-Data-Protection-Regulation-Information-Sheet.pdf.

Feedback request – profiling and automated decision-making. (2017). [ebook] Information Commissioner's Office. Available at: https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf.

González Fuster, G., Gutwirth, S. and Ellyne, E. (2010). *Profiling in the European Union: A high-risk practice*. [ebook] INEX POLICY BRIEF NO. 10. Available at: https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf.

Goodman, B. and Flaxman, S. (2016). *European Union regulations on algorithmic decision-making and a "right to explanation"*. 3rd ed. [pdf] New York: University of Oxford. Available at: https://arxiv.org/pdf/1606.08813.pdf.

Guidance on Political Campaigning. (2017). [ebook] ICO. Available at: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf.

Online Profiling: A report to Congress. (2000). [pdf] Federal Trade Commission. Available at: https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress/onlineprofilingreportjune2000.pdf.

Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. (2000). [pdf] Federal Trade Commission. Available at: https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission.

Schipper, B. and Woo, H. (2017). *Political Awareness, Microtargeting of Voters, and Negative Electoral Campaigning*. [pdf] University of California. Available at: http://faculty.econ.ucdavis.edu/faculty/schipper/polaw.pdf.

Staff Report (2009). *Self-regulatory Principles for online behavioral advertising*. [pdf] Federal Trade Commission. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

Vibhute, K. and Aynalem, F. (2009). *Legal Research Methods*. [ebook] Chilot Wordpress. Available at: https://chilot.files.wordpress.com/2011/06/legal-research-methods.pdf.

Journal articles

Bennett, C. (2013). The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. *First Monday*, [online] 18(8). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4789.

Bennett, C. (2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, [online] 6(4), pp.261-275. Available at: https://academic.oup.com/idpl/article/6/4/261/2567747.

Berger, D. (2014). Balancing Consumer Privacy with Behavioral Targeting. *Santa Clara Computer and High Technology Law Journal*, [online] 27(3), pp.3-61. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1693029.

Breen, O. (2008). EU Regulation of Charitable Organizations: The Politics of Legally Enabling Civil Society. *The International Journal of Not-for-Profit Law*, [online] 10(3). Available at: http://www.icnl.org/research/journal/vol10iss3/special_3.htm.

Bygrave, L. (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Report*, [online] 17, pp.17-24. Available at: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf.

Casey, J. (2016). Comparing Nonprofit Sectors Around the World: What Do We Know and How Do We Know It?. *Journal of Nonprofit Education and Leadership*, [online] 6(3), pp.187- 223. Available at: http://js.sagamorepub.com/jnel/article/view/7583.
Castelluccia, C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. In: S. Gutwirth, ed., *European Data Protection: In Good Health?,*. Springer, pp.21-33.

Clarke, R. (1993). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law and Information Science*, [online] 4(2), pp.403-419. Available at: http://heinonline.org/HOL/Page?handle=hein.journals/jlinfos4&div=33&g_sent=1&casa_token=&collection=journals#.

De Hert, P. and Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, [online] 28(2), pp.130-142. Available at: https://www.sciencedirect.com/science/article/pii/S0267364912000295.

Eskens, S., Helberger, N. and Moeller, J. (2017). Challenged by news personalisation: five perspectives on the right to receive information. *Journal of Media Law*, 9(2), pp.259-284.

Gandomi, A. and Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, [online] 35(2), pp.137-144. Available at: http://www.sciencedirect.com/science/article/pii/S0268401214001066?via%3Dihub.

Helberger, N. (2016). Policy Implications From Algorithmic Profiling and the Changing Relationship Between Newsreaders and the Media, *Journal of the European Institute for Communication and Culture,* [online] 23(2), pp.188-203. Available at http://www.tandfonline.com/doi/full/10.1080/13183222.2016.1162989.

Helberger, N. (2016). Policy Implications From Algorithmic Profiling and the Changing Relationship Between Newsreaders and the Media. *Javnost - The Public*, [online] 23(2), pp.188-203. Available at: http://www.tandfonline.com/doi/full/10.1080/13183222.2016.1162989.

Howard, P. and Kreiss, D. (2010). Political parties and voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective. *First Monday*, [online] 15(12). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595120.

Kreiss, D. (2012). Yes We Can (Profile You) A Brief Primer on Campaigns and Political Data. *Stanford Law Review*, [online] 66(70), pp.70-74. Available at: https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/.

Kreiss, D. and Howard, P. (2010). New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era. *International Journal of Communication*, [online] 4, pp.1032-1050. Available at: http://ijoc.org/index.php/ijoc/article/view/870/473.

Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*. [online], pp.1-15. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781.

Marx, G. (1984). Routinizing the Discovery of Secrets- Computers as Informants. *American Behavioral Scientist*, [online] 27(4), pp.423-452. Available at: http://journals.sagepub.com/doi/abs/10.1177/000276484027004003#articleCitationDownloadContainer.

Neely, S. (2003). Non-Profits, Not-for-Profits, and Charities: What's the Difference?. *The Scrivener*, [online] 12(3), pp.11-12. Available at: https://www.notaries.bc.ca/resources/scrivener/fall2003/12_3_5.pdf.

Poullet, Y. (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review*, [online] 22(3), pp.206-217. Available at: https://www.sciencedirect.com/science/article/pii/S0267364906000318.

Rubinstein, I. (2014). Voter Privacy in the Age of Big Data. *Wisconsin Law Review*. [online] pp.861-936. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447956.

Rubinstein, I., Lee, R. and Schwartz, P. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review*, [online] 75(1), pp.261-286. Available at: http://scholarship.law.berkeley.edu/facpubs/1497/.

Rustin-Paschal, N. (2011). Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues. *William & Mary Bill of Rights Journal*, [online] 19(4), pp.906-925. Available at: http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1583&context=wmborj.

Schermer, B. (2011). *The limits of privacy in automated profiling and data mining*. [online] Computer Law & Security Review, Volume 27, Issue 1, pp.45-52. Available at: http://www.sciencedirect.com/science/article/pii/S0267364910001767.

Solove, D. and Schwartz, P. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, [online] 86(6), pp.1814-1894. Available at: http://heinonline.org/HOL/Page?handle=hein.journals/nylr86&div=50&g_sent=1&casa_token=&collection=journals.

van der Sloot, B. and van Schendel, S. (2016). Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study. *JIPITEC*, [online] 7(3), 110 para 1. Available at: http://www.jipitec.eu/issues/jipitec-7-2-2016/4438.

Veale, M. and Edwards, L. (2017). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. *Computer Law & Security Review*, [online] Forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071679.

Legislation

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119.

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, OJ L 281, 23/11/1995, pp.0031-0050.

H.R.3618 - 112th Congress (2011-2012): End Racial Profiling Act of 2011. [online] Available at: https://www.congress.gov/bill/112th-congress/house-bill/3618?resultIndex=5.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003 (COD). 10 January 2017. Available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

Reports and guidelines

Article 29 Data Protection Working Party. Advice paper on special categories of data (“sensitive data”). 20 April 2011. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 3 October 2017. WP251. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=47742.

Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679. WP 260. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=47741.

Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 4 April 2017, WP247. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Draft Albrecht report, amendment 162, article 20(3)), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

Websites and blogs

Aggregateiq.com. (2017). [online] Available at: https://aggregateiq.com/.

Angwin, J. and Larson, J. (2017). *Help Us Monitor Political Ads Online — ProPublica*. [online] ProPublica. Available at: https://www.propublica.org/article/help-us-monitor-political-ads-online.

Ca-political.com. (2017). *CA Advantage | CA Political*. [online] Available at: https://ca-political.com/ca-advantage.

Ca-political.com. (2017). *Donald J. Trump for President*. [online] Available at: https://ca-political.com/index.php/casestudies/casestudydonaldjtrumpforpresident2016.

Ca-political.com. (2017). *Services | CA Political*. [online] Available at: https://ca-political.com/services.

Davies, H. (2016). *Ted Cruz erased Trump's Iowa lead by spending millions on voter targeting*. [online] the Guardian. Available at: https://www.theguardian.com/us-news/2016/feb/01/ted-cruz-trump-iowa-caucus-voter-targeting.

Denham, E. (2017). The Information Commissioner opens a formal investigation into the use of data analytics for political purposes. [Blog] *Information Commissioner's Office blog*. Available at: https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/.

Denham, E. (2017). Update on ICO investigation into data analytics for political purposes. [Blog] *Information Commissioner's Office blog*. Available at: https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/#more-3192.

Doward, J. (2017). *Did Cambridge Analytica influence the Brexit vote and the US election?*. [online] the Guardian. Available at: https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump.

EU GDPR Portal. (2017). *Home Page of EU GDPR*. [online] Available at: https://www.eugdpr.org/.

Eyeonelections.com. (2016). *Project DATA | Digital Ad Tracking and Analysis*. [online] Available at: http://www.eyeonelections.com/.

Falchetta, T. (2017). *Hiding in plain sight—political profiling of voters*. [online] Privacy International. Available at: https://privacyinternational.org/node/1460.

Freeze, C. (2017). *B.C., Britain investigate role of Canadian tech firm AggregateIQ in Brexit vote*. [online] The Globe and Mail. Available at: https://www.theglobeandmail.com/news/national/bc-britain-investigate-role-of-canadian-tech-firm-aggregateiq-in-brexit-vote/article37340241/.

Funk, M. (2016). *Opinion | The Secret Agenda of a Facebook Quiz*. [online] Nytimes.com. Available at: https://www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html.

Goodin, D. (2013). *FBI warns hacking spree on government agencies is a "widespread problem"*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2013/11/fbi-warns-hacking-spree-on-government-agencies-is-a-widespread-problem/.

Grassegger, H. and Krogerus, M. (2017). *The Data That Turned the World Upside Down*. [online] Motherboard. Available at: https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win.

Hamburger, T. (2015). *Cruz campaign credits psychological data and analytics for its rising success*. [online] The Washington Post. Available at: https://www.washingtonpost.com/politics/cruz-campaign-credits-psychological-data-and-analytics-for-its-rising-success/2015/12/13/4cb0baf8-9dc5-11e5-bce4-708fe33e3288_story.html?utm_term=.d4ac51b9e4c8.

Ico.org.uk. (2017). *Political campaigning practices*. [online] Available at: https://ico.org.uk/for-the-public/political-campaigning-practices/.

Kaye, K. (2016). *In D.C., Cambridge Analytica Not Exactly Toast of the Town*. [online] Adage.com. Available at: http://adage.com/article/campaign-trail/cambridge-analytica-toast/305439/.

LII / Legal Information Institute. (2017). *First Amendment*. [online] Available at: https://www.law.cornell.edu/constitution/first_amendment.

Maass, D. (2017). *Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election | Electronic Frontier Foundation*. [online] Available at: https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election.

Major, K. (2017). *Facebook 'dark ads' will win this election for the Tories - but there's something you can do about it*. [online] The Independent. Available at: http://www.independent.co.uk/voices/election-facebook-dark-targeted-ads-tories-labour-do-something-a7745341.html.

McClenaghan, M. (2017). *The "dark ads" election: How are political parties targeting you on Facebook?*. [online] The Bureau of Investigative Journalism. Available at: https://www.thebureauinvestigates.com/stories/2017-05-15/the-dark-ads-election-how-are-political-parties-targeting-you-on-facebook.

Research Now. (2017). *Research Now: U.S. Voter and Political Market Research*. [online] Available at: https://www.researchnow.com/products-services/global-audiences-and-panel/political-panel/?lang=gb.

Solon.barocas.org. (n.d.). *Soap Box | Solon Barocas*. [online] Available at: http://solon.barocas.org/?page_id=38.

Think with Google. (2017). *How Political Ads and Video Content Influence Voter Opinion*. [online] Available at: https://www.thinkwithgoogle.com/marketing-resources/content-marketing/political-ads-video-content-influence-voter-opinion/.

Think with Google. (2017). *What Marketers Can Learn From the Latest Data About Voter Behavior Online*. [online] Available at: https://www.thinkwithgoogle.com/consumer-insights/marketer-lessons-online-voter-behavior-data/.

Uk.practicallaw.thomsonreuters.com. (2017). [online] Available at: https://uk.practicallaw.thomsonreuters.com/4-385-3476?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

Webtap.princeton.edu. (2018). *Princeton WebTAP – Web Transparency & Accountability Project @ Princeton*. [online] Available at: https://webtap.princeton.edu/.

WhatIs.com. (2017). *What is geo-fencing (geofencing)? - Definition from WhatIs.com*. [online] Available at: http://whatis.techtarget.com/definition/geofencing.

Who Targets Me?. (2017). *About us - Who Targets Me?*. [online] Available at: https://whotargets.me/en/about/.

Winningcampaigns.org. (2017). *Winning Campaigns : Learn From The Experts Articles : Micro-Targeting: New Wave Political Campaigning*. [online] Available at: http://www.winningcampaigns.org/Winning-Campaigns-Archive-Articles/Micro-Targeting-New-Wave-Political-Campaigning.html.

Zanfir-Fortuna, G. (2016). *A look at political psychological targeting, EU data protection law and the US elections*. [online] pdpEcho. Available at: https://pdpecho.com/2016/11/14/does-eu-data-protection-law-apply-to-the-political-profilers-targeting-us-voters/.

Working papers, reports, conference proceedings and other miscellaneous sources

AMAPOLA, UNICRI, Tilburg University (2014). *Defining Profiling*. [online]. Available at: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf.

Barocas, S. (2012). The price of precision: voter microtargeting and its potential harms to the democratic process. In: *Conference on Information and Knowledge Management*. [online] ACM, pp.31-36. Available at: https://dl.acm.org/citation.cfm?id=2389671.

Borgesius, F. (2017). *Improving privacy protection in the area of behavioural targeting*. Ph.D. University of Amsterdam, Faculty of Law (FdR), Institute for Information Law (IViR).

Dinant, J.M., Lazaro, C., Poullet, Y., Lefever, N. and Rouvroy, A. (2008). Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD), Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, 11 January, Strasbourg.

Douwe, K. (2012). Comments on Selected Topics in the Draft EU Data Protection Regulation. [online]. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2150145.

Kuehn, A. and Mueller, M. (2012). *Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States*. [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181.

Leenes, R. (2009). Reply by Ronald Leenes (TILT): Addressing the Obscurity of Data Clouds. TILT Law & Technology Working Paper No. 012/2009; Tilburg University Legal Studies Working Paper No. 008/2009. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1393193.

PROtecting citizens' rights and Fighting ILlicit profilING (PROFILING) project (2014). *Profiling- Protecting citizen's rights, fighting illicit profiling*. [online]. Available at: http://www.unicri.it/news/files/Profiling_final_report_2014.pdf.

Resolution on profiling. (2013). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf.

Resolution on the Use of Personal Data for Political Communication. (2005). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf.

Soziologe.guagnin.de. (2014). *PROFILING | PROtecting citizens' rights Fighting ILlicit profilING*. [online] Available at: http://soziologe.guagnin.de/profiling-project.eu/index.html%3Fp=6.html.

Turow, J., Delli Carpini, M. X., Draper, N. A., & Howard-Williams, R. (2012). Americans Roundly Reject Tailored Political Advertising. Annenberg School for Communication, University of Pennsylvania. Available at http://repository.upenn.edu/asc_papers/.

Uruguay Declaration on profiling. (2012). In: *International Conference of Data Protection and Privacy Commissioners*. [online] Available at: https://edps.europa.eu/sites/edp/files/publication/12-10-26_uruguay_declaration_profiling_en.pdf.