January 2021

MICRO-TARGETING IN POLITICAL CAMPAIGNS: A comparative analysis of legal frameworks

THE UNIVERSITY of EDINBURGH
Edinburgh Law School

THE UNIVERSITY *of* EDINBURGH
Edinburgh Law School

Authors

This report was compiled under the direction of Dr Paolo Cavaliere, Lecturer in Digital Media and IT Law, University of Edinburgh Law School, in collaboration with Privacy International.

Find out more about Edinburgh Law School's research at:
https://www.law.ed.ac.uk/research.

Researchers:

Paolo Cavaliere
Hashim Mude
Iona Bonaventura
Mariana Galindo Sanchez

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Photo by Possessed Photography on Unsplash

CONTENTS

EXECUTIVE SUMMARY

This paper examines the various legal frameworks governing micro-targeting in political campaigns in 6 states: Canada, Brazil, France, Italy, Spain and the UK. It aims to assess national practices as well as point out gaps in their respective frameworks. The paper commences by examining how micro-targeting is defined and thereafter examines the legal provisions applicable to micro-targeting activities.

Defining micro-targeting

There is no clear statutory definition of the practice in any of the 6 states. Micro-targeting is in fact the culmination of a series of activities which are themselves most often well-defined and regulated (such as collecting of personal data, using the data for profiling and transmitting personalised communications to individual voters). As a result, the legal frameworks governing political micro-targeting are most often piecemeal provisions relating to different aspects of data protection, privacy and electoral law, which in turn present a number of gaps and loopholes that campaigns can easily exploit.

Collection of personal data

Access to personal data is a fundamental pre-condition for campaigns and advertisers to engage in micro-targeting practices. As a first step, campaigns typically collect the so-called identifiers, i.e. the data that uniquely identify an individual such as for instance the name or the address. Such data can be obtained through a number of channels, although by far the most common way is through electoral registers.

The analysis revealed a lack of consistency across the board with respect to how information from electoral registers is made available to third parties. At

one end of the spectrum, voters' lists are widely accessible to different groups under a range of purposes – the UK being a leading example –, whereas in other cases it is possible to observe a generalised trend towards limiting access to the registers. Barring access to commercial entities is now common practice, while political entities in different forms remain widely allowed to access the information contained in the lists, either in full or at least in part. The cases of France, where the law has devised a dynamic test to assess the reasons supporting a request to access electors' lists and their commercial nature, and Canada, where the law provides a static definition of legitimate purposes to access the lists and makes an offence of the others, are examples of the possible different approaches that law-makers can resort to.

However, these measures are unfortunately far from enough – largely for two reasons. Firstly, it proves difficult to strike a suitable balance between competing interests: the growing awareness of the risks related with data exploitation need to be balanced out against the principle of openness of the electoral process, and the legitimate interest of parties and campaigns to engage with voters in fulfilment of their own right to freedom of expression and the public's right to receive information relevant to the political debate. Second, the current dynamics of micro-targeting concern a much broader range of personal data than those traditionally considered essential or relevant in the political context, some of which is granted enhanced protection. Detailed information revealing general interests and behaviours is increasingly relied upon in order to develop more individualised profiles.

Data from the electoral register acts as a 'spine' on which to add more granular information from other sources. Collection of this additional data, while not prohibited, is hindered by the GDPR (applicable to Italy, France and Spain) as it likely requires the consent of the data subject and imposes a data minimisation principle which would be breached by a blanket collection of personal data. Spanish law is particularly restrictive, as an impact assessment report and an advisory report from the DPA may be required for such data collection. In Brazil, processing personal data also requires consent by the data subject. Canadian privacy laws do not apply to political parties (except for the province of British Columbia) which are only subject to a special regime that requires them to

submit and publish policies for protecting personal information. They are not subject to minimum standards and their practices are not subject to oversight by an independent body. Collection of personal data within British Columbia requires the consent (with a few exceptions) of the data subject.

The collection of data on individuals' lifestyle is a relative novelty in the field of political communication, and most of the available regulation and guidance in this respect comes from data protection authorities' guidelines and other soft-law sources. The practical measures introduced by the different authorities change even significantly from one case to another, although some trends can be observed across the countries considered in this study. The leeway granted to political organisations seems to be generally narrowing down, as authorities are now evidently paying attention and expect parties and campaigns to comply with more stringent procedures. There is an increasing emphasis on the transparency of data collection: the purpose of using data for political communications is now generally expected to be communicated explicitly, even in case the data is collected from third parties, and the subject's consent cannot be normally implied. Two general models seem to emerge from a comparative perspective, with a major divide between those countries that exclude the possibility of processing some categories of data even with the subject's consent, and others that instead consider consent a lawful ground for processing any categories of data.

Using the data for profiling

Using the collected data to infer information about voters is not prohibited but would in most cases require explicit consent under the GDPR, in those countries that are EU Member States. The DPAs in the UK and Italy have developed detailed guidance in this area. The Italian DPA emphasises the informed consent of the data subject through simplifying consent notices. In France data cross-matching and profiling likely requires consent, while Spain appears to entirely ban the processing of sensitive personal data even with the consent of the data subject. France and Spain stand out amongst the EU countries for a lack of

guidance from their DPAs in this area. In Brazil, the processing of sensitive personal data requires express consent. Canadian privacy laws would also likely require the consent of the data subject for profiling, but these provisions do not apply to political parties outside of British Columbia.

At this stage of the process, the countries considered show a significant degree of diversification in their respective approaches. Most notably, significant differences exist between countries whose data protection authorities have provided relevant guidance, in a more or less detailed form, and others where the relevant framework is largely silent on the issue. Other differences emerge in the role played by the data subject's consent, in some cases a sufficient legal basis for cross-matching but not in all the countries examined, and the need for detailed guidance as to the different aims and circumstances that lead to situations where cross-matching would not be allowed or the controller would need to comply with further requirements – a profile in which respect several of the frameworks examined seem to lack of clarity at present.

Sending out tailored messages (Micro-targeting)

The final step in micro-targeting is the sending out of tailored messages. It is not prohibited in any of the countries nor is it subject to specific consent requirements. Rather, all the countries have adopted measures to improve transparency. These provisions vary in both scope and efficacy but largely seek to enable voters to easily identify political advertisements as well as the identity of the senders.

In Spain all electoral messaging is to be explicitly labelled as such and the sender's identity is to be provided. French law contains a similar provision though it only applies three months before a general election month. In Brazil political advertisements are to be clearly identified and can only be contracted by political parties, candidates or their representatives. In the UK electoral publications that are printed must identify the source and the government has committed itself to an "imprint requirement" that would compel online campaign

material to show where an advertisement has come from and how it has been funded. Canada has adopted a novel approach and has created a single, publicly available and searchable, online database of political adverts that have been published on online platforms.

Although each legal jurisdiction has taken a different approach to improving the transparency of political direct marketing online, it is clear that such personalised communications must be suitably transparent for recipients to fully understand their nature and origin. The most common means of ensuring such transparency is through the introduction of an 'imprint requirement' for online political ads. However, such a requirement must be properly drafted and cover election material at all times, not only during a specific campaigning period. An alternative and most promising method which has been used successfully in Canada is the introduction of a database where members of the public can readily access information on any online advertising messages.

1 INTRODUCTION

Direct marketing has significant potential for being used as an exploitative form of digital campaigning because the origins of personalised communications is often unclear. Targeted messages may be disseminated by a wide range of actors – campaigners posing as individuals, fake social media accounts, or automated software programs ('bots') – without the recipient being aware that these messages are part of a political campaign.[1]

The use of direct marketing by political campaigns can be particularly difficult to trace when carried out through social media platforms. "List-based" targeting tools, for instance, are widely made available by social media platforms to advertisers (including political campaigns) allowing them to match any lists of data they may already have (such as for instance email addresses of supporters) with the platform's own user database.[2] This enables political messages to be sent via social channels where recipients are less readily able to identify the source of communications.[3] The use of "lookalike" tools enables campaigns to communicate with a wider audience based on the characteristics of the original "list-based" group without requisite consent.[4] "Viral marketing" (or "tell a friend" campaigns) in particular make it difficult for targeted individuals to recognise the true nature of political messages or posts being shared online.[5]

Recent major initiatives taken at either the national or supranational level have admittedly demonstrated an increasing concern from multiple quarters to increase the transparency of data-driven political advertising. From a comparative perspective, most European countries require that political

[1] Electoral Commission, Digital Campaigning – increasing transparency for voters, 13 August 2019, available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters
[2] See Information Commissioner's Office, 'Direct marketing code of practice. Draft code for consultation', 90.
[3] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019 at p.89
[4] Privacy Commissioner for British Columbia, Full Disclosure: Political Parties, Campaign Data, and Voter Consent', 2019, B.C.I.P.C.D. No. 07 26 https://www.oipc.bc.ca/investigation-reports/2278
[5] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019 at p.79

advertising on traditional media is 'properly identified and labelled as such'.[6] The emphasis on transparency has been also reprised in the most relevant examples of such recent efforts at the EU level, the Communication on Tackling online disinformation[7] and the Code of Practice on disinformation, which indeed require digital platforms, amongst other commitments, to implement policies against misrepresentation, prioritise authentic information, close fake accounts and mark bots' activities.

Although some social media platforms have attempted to develop their own political advertising standards, these efforts have been criticised for 'lacking teeth and being easy to subject by bad actors'.[8] The Code of Practice has been described as a 'a fairly messy and in some ways structurally incoherent document'[9] most likely to prove ineffective, for the reason, amongst others, that it treats the issue of disinformation as one of malicious content, and as such is '[i]t cannot and will not capture all malicious content … it can't prevent all – or perhaps even most – of the worst instances of "viral deception."'[10]

In light of the difficulties and limitations of content governance, there is an urgent need to focus on those practices that fuel it and enable disinformation to spread, such as the systematic collection of vast amounts of data, individual profiling and targeted communications.[11] In this study, we present a comparative analysis of six different national approaches with regard to the regulation of data-driven targeting and political campaigns, in the spirit of highlighting some emerging common trends and some persisting gaps, as well as some unique features of the systems considered.

---

[6] Iva Nenadić, 'Unpacking the "European approach" to tackling challenges of disinformation and political manipulation' (2019) 8 Internet Policy Review 1, 4.
[7] European Commission, Tackling online disinformation: a European Approach, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2018/236.
[8] Open Rights Group, *Imprints: who's responsible?*, 31 March 2020, available at: https://www.openrightsgroup.org/blog/2020/imprints-who's-responsible.
[9] Peter H Chase, 'The EU Code of Practice on Disinformation: The Difficulty of Regulating a Nebulous Problem', 14. Working paper of the Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 2019 available at: https://www.ivir.nl/publicaties/download/EU_Code_Practice_Disinformation_Aug_2019.pdf.
[10] *Ibid.*
[11] Privacy International, 'Challenging Data Exploitation in Political Campaigning: PI Recommendations', June 2020, pp 7-9, available at: https://privacyinternational.org/sites/default/files/2020-06/PI%20Recs_Challenging%20Data%20Exploitation%20in%20Political%20Campaigning.pdf.

After a brief overview of how micro-targeting is defined in the different countries considered in this study (i.e. Brazil, Canada, France, Italy, Spain and the UK), the analysis focuses on the legal frameworks regulating a range of activities that, each in a different way, contribute to allowing for the exploitation of individual data and micro-targeting practices, such as accessing voters' identifiers from the electoral registers; collecting data on the individual's lifestyle; data profiling and cross-matching; the delivery of personalised communications. Due to its complex, multi-faceted nature, political micro-targeting is difficult to regulate with a single, comprehensive legal framework – as indeed none of the countries examined does. Instead, the relevant provisions are usually to be found across multiple statutes or regulations, variably relating to different aspects of data protection, electoral campaigns and general media and communications law, often adding a further element of opacity to understanding which types of conduct are allowed and which are not. The lack of clear and easily accessible regulatory frameworks poses a risk in that any regulatory gaps could be exploited by platforms or campaigns.

2 DEFINING THE ISSUE OF 'MICRO-TARGETING'

As micro-targeting practices emerge at the global level, one apparent difficulty is that the field of political advertising has been traditionally regulated in strikingly different manners across different countries. Even within the EU and in relation to traditional media, definitions of 'political advertising' can change significantly from one Member State to another[12] and a common framework is not included in the recently revised AudioVisual Media Services Directive or other similar provisions. [13]

Against this background, the lack of clear statutory definition of micro-targeting in any of the six countries subject of this analysis is hardly surprising. However, the Data Protection Authorities ('DPAs') in the UK and Canada have sought to explain what the term encompasses. The information Commissioners Office in the UK (ICO, UK) has defined it as:

> *'a form of online* targeted *advertising that analyses personal data to identify the interests of a specific audience or individual in order to influence their actions. Microtargeting may be used to offer a personalised message to an individual or audience using an online service such as social media. Microtargeting may determine what and how relevant content is delivered to an individual online and is sometimes used to market goods or services and for political marketing'.*[14]

This definition has been relied on by the Scottish Law Commission and the Law Commission for England and Wales.[15]

[12] Christina Holtz-Bacha, 'Regulation of Electoral Advertising in Europe' in Christina Holtz-Bacha, Edoardo Novelli and Kevin Rafter (eds), *Political Advertising in the 2014 European Parliament Elections* (Palgrave Macmillan, London 2017) 27, 29-30.
[13] https://ec.europa.eu/digital-single-market/en/audiovisual-media-services-directive-avmsd
[14] ICO, *Microtargeting*, https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/
[15] Law Commission and Scottish Law Commission, *Electoral Law: A joint final report*, law Com No. 389, Scot Law Com No 256, 16 March 2020, at p.156 para 12.36,

The Office of the Privacy Commissioner of Canada (the DPA at the federal level) commissioned a report that referred to micro-targeting as 'refined segmentation according to a host of demographic and attitudinal variables'.[16] The Office of the Information and Privacy Commissioner for British Columbia (DPA at the district level) describes it as the type of targeting occuring 'when a very narrow and highly specific category of people are chosen as an advertising target'.[17]

In France, Spain and Italy there are only indirect references to micro-targeting. Firstly, at an EU level, the European Data Protection Supervisors (EDPS) opinion on online manipulation and personal data refers to the practice of micro-targeting as consisting of 'a more personal message to a segment of people sharing certain traits or even potentially determine the prices for products or services. It may consist in how social media platforms determine which content that appears on individual news feeds and in what order.'[18]

The EU Commission guidance on the application of Union data protection law in the electoral context refers to offering 'a personalised message to an individual or audience using an online service e.g. social media.' [19]

At a national level, the French DPA has described it as a 'challenging' practice[20] and the Spanish DPA has referred to it as a form of 'unproportional data processing' but neither have defined the term.[21] The DPA in Italy has included two

https://www.scotlawcom.gov.uk/files/9215/8411/2303/Electoral_Law_-_A_joint_final_report_Report_No_256.pdf

[16] CJ Bennett and RM Bayley, 'Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis' (2012) Privacy Research Papers: Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp

[17] 'INVESTIGATION REPORT P19-01 Full Disclosure: Political Parties, Campaign Data, and Voter Consent' (Privacy Commissioner for British Columbia 2019) B.C.I.P.C.D. No. 07 25 <https://www.oipc.bc.ca/investigation-reports/2278> accessed 10 May 2020. https://www.oipc.bc.ca/investigation-reports/2278

[18] Opinion 3/2018 of the European Data Protection Supervisor (EDPS) on online manipulation and personal data, 9.

[19] European Commission - Commission guidance on the application of Union data protection law in the electoral, 7.

[20] 'Communication Politique : Quelles Sont Les Règles Pour l'utilisation Des Données Issues Des Réseaux Sociaux ? | CNIL' <https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux> accessed 2 July 2020.

[21] Article 6 (1). Circular 1/2019 (entered into force on 11 March 2019) of the Spanish Data Protection Agency (Agencia Española para la Protección de Datos (AEPD)), on the processing of personal data relating to political opinions and the sending of electoral propaganda by electronic means or systems of

types of processing in its DPIA list (issued pursuant to Art 35(4) GDPR) that conceivably cover micro-targeting:

> *'Large-scale evaluation or scoring, as well as any type of processing involving data subjects'* profiling or predicting aspects concerning *'the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, performed on-line or on apps.'*[22]

And

> *'Any processing that entails the systematic use of data to observe, monitor or control data subjects, including the collection of data through networks, including when performed on-line or on apps, and the processing of unique identifiers that may be used to identify users of information society services, including web services, interactive TV, etcetera, with regard to consumption patterns and viewing data over extended periods. Processing of metadata, e.g. in the fields of telecommunications, banking etcetera, performed for profiling purposes or more in general for organisational, budgetary prediction, technology upgrade, network improvement, fraud prevention, anti-spam and security services, etcetera are also included in this category.'*[23]

In Brazil there is no clear definition of micro-targeting but the term 'boost content' appears to convey a similar meaning.[24] It refers to 'the mechanism or

messaging by political parties, federations, coalitions and groups of voters under Article 58 bis of LOREG.

[22] Garante per la Protezione dei Dati Personali, 'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018', para 1, available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979

[23] Ibid., para 3.

[24] Though this interpretation is subject to challenge as the Brazilian DPA who would have provided guidance on the meaning of the term is yet to be constituted.

service that, through contracting with Internet application providers, enhances the reach and dissemination of information to reach users who would not normally have access to its content, including among the forms of boost content the paid prioritization of content resulting from Internet search applications'.[25]

2.1. IS DEFINING THE TERM IMPORTANT?

The lack of a clear statutory definition in these six countries is addressed either directly by the DPA's defining it (Spain, UK and Canada) or indirectly through the use of analogous terms (Brazil, France and Italy). The lack of a precise definition (both at the domestic level and in a comparative perspective) may not necessarily frustrate the purpose of regulating the phenomenon effectively, as long as the single activities associated with it are already covered by law.

Micro-targeting, whether used as a marketing technique for products and services or in political campaigns, involves three steps: the collection of personal data, using the data for profiling and then sending out tailored messages. As the analysis in the next sections of this study will demonstrate, the first two steps of micro-targeting are generally defined and regulated by national policy- and law-makers and, as a result, the definition and regulation of the final step (micro-targeting) could appear superfluous.

However, the analysis will also illustrate how micro-targeting practices in the political arena have their own specificities, as they stem from different motives than those deployed with purely commercial interests and are likely to impinge on fundamental rights in a different way.

The more pertinent question therefore is whether to define and enact specific rules in relation to political micro-targeting as this activity generates greater

[25] art. 26, § 2 of Electoral Law (Law 9.504 of 30 September of 1997)

concerns when deployed in political campaigns than when it is used to market products or services.

While its use in both fields creates significant privacy concerns, the former has the potential to significantly impair the functioning of a democracy. It has been argued that political micro-targeting can have direct effects such as voter manipulation and suppression, aggravate polarisation, perpetuate misinformation and have indirect long-term effects by incentivising political parties to ignore people that they deem are unlikely to vote leading to 'increased levels of voter disengagement and lower turnout' and the resulting underrepresentation of groups of people.[26]

If this is the case, then it stands to reason that it may be important to develop specific rules for the use of micro-targeting in political campaigns rather than rely on general data protection laws. This would require a working definition of the term. However as has been noted elsewhere 'adopting such rules would be difficult for the EU, as different EU member states have different traditions in the context of elections' and such steps may therefore have to be taken at a national level.[27]

[26] Frederik J Zuiderveen Borgesius et Al., 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14 *Utrecht Law Review* 87
[27] Tom Dobber et Al., 'The regulation of online political micro-targeting in Europe' (2019) 8 *Internet Policy Review*

3 ACCESS TO VOTERS' IDENTIFIERS FROM THE ELECTORAL REGISTER

Access to personal data is a fundamental pre-condition for campaigns and advertisers to engage in micro-targeting practices. As a first step, campaigns typically collect the so-called identifiers, i.e. the data that uniquely identify an individual such as for instance the name or the address. Such data can be obtained through a number of channels, including for instance directly from the voters, in the course of surveys or canvassing, although by far the most common way is through the electoral register. Access to identifiers is key to beginning the process of harnessing the potential of data for micro-targeting.

In the EU, the collection and processing of such data is covered by the GDPR, particularly Article 5 principles of 'lawfulness, fairness and transparency', 'purpose limitation' and 'data minimisation' are particularly relevant. Moreover, the kind of data that would be collected in any effective micro-targeting campaign such as racial or ethnic origin, political opinions, religious or philosophical beliefs are considered to be a special category of personal data whose processing save for a few exceptions is prohibited. One such exception under Article 9 (2)(d) allows political parties to process this data provided it relates to their members or former members who 'have regular contact with it' but they are prohibited from disclosing such data to outside bodies without the consent of the data subject.

Micro-targeting in Europe is hindered at the first stage as it is difficult to collect data about people.[28] The two countries not covered by the GDPR (Canada[29] and Brazil[30]) have similar provisions in their data protection laws. Nonetheless,

[28] Tom Dobber et Al., 'The regulation of online political micro-targeting in Europe' (2019) 8 Internet Policy Review.
[29] S. 6, 10-12 Personal Information Protection Act of British Columbia; S. 5, Schedule 1 Personal Information Protection and Electronic Documents Act.
[30] Article 5, 6 & 11 Law 13.709 of 14 August 2018 (General Data Protection Law in Portuguese, Lei Geral de Proteção de Dados Pessoais (LGPD) .

relevant data is still accessible through a range of sources in the public domain, including electoral registers.

3.1 THE INFORMATION INCLUDED IN ELECTORAL REGISTERS

Despite the increasingly restrictive frameworks offered by data protection laws at the national or supranational level, the collection of individual data remains lawful in a number of circumstances, most commonly – in the context of political communications – through surveys and canvassing, or via electoral registers.

Information included in the electoral registers has slight variations from a country to another, ranging from a minimum core including such as their names, address, and electoral number in the UK;[31] to which other countries add further information useful to identify voters and their demographics, like their date and place of birth in France[32] and Italy.[33] In Spain, the Electoral Census adds to all these a further requirement such as national identity number[34] while the inclusion of any further specific information is forbidden by the law.[35] The Canadian federal law requires electoral registers to include all this information alongside an identification document containing photograph and service number[36] and any other information that the Chief Electoral Officer considers necessary.[37] However, laws at provincial level can require different information: in the province of Alberta, the register includes details of gender, citizenship and date

[31] Representation of the People Act 1983 s.9(5-6).
[32] Electoral Code, Article L. 16.
[33] Decreto del Presidente della Repubblica no. 223/1967, Art 5.
[34] article 32(1) LOREG.
[35] Article 41(2) LOREG.
[36] S. 211.2(4).
[37] S.49(2).

of birth,[38] addresses, postal codes and telephone numbers[39] although the law limits the purpose of such details to verifying the list when revising the register.[40] Provincial law in British Columbia allows to omit or conceal voter information in order to protect privacy or security.[41]

It is worth noting that some countries have different versions of electoral registers: in the UK, for instance, there are two versions of the electoral register: the full register and the open (edited) register. Access to voters' identifiers differs between these two registers:[42] the full register includes names and address of everyone who is registered to vote, unless an individual decides to register to vote anonymously,[43] whereas the edited register contains only the names and addresses of those electors who have not opted out of it, either at the time of applying for registration,[44] or by notifying the registration officer.[45] In Canada exist both a Register of Electors, which lists any persons currently qualified as electors, and a Register of future Electors Canadian which lists citizens aged between 14-17. It is entirely voluntary and the information is not shared with political parties.[46] A further distinction exists between preliminary and official list of electors; the former includes only the name and address of each elector in the electoral district and the identifier,[47] whereas the latter also includes information of each electors' polling division[48] and is made available to each registered or eligible (i.e. a party that has satisfied the criteria for registration but has not yet registered) party that request them and to each candidate for their respective electoral district.[49]

[38] Elections Act (Alberta) S.13 (2).
[39] S. 17
[40] S.13(3) and S.17(3).
[41] Election Act (British Columbia) s. 51 (4).
[42] Information Commissioner's Office, "Guidance on political campaigning: draft framework code for consultation", 2019, at p.50 available at: https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf
[43] The Electoral Commission, *The electoral register*, 6 April 2020, available at: https://www.electoralcommission.org.uk/i-am-a/voter/electoral-register
[44] r.26(1)(h) RP(S)R and RP(E/W)R; r.27(1)(f) RP(NI)R
[45] r.93A(1) RP(S)R and RP(E/W)R
[46] Elections Canada, 'FAQs about the Register of Future Electors' <https://www.elections.ca/content.aspx?section=vot&dir=faq&document=faqfut&lang=e#gen1> accessed 27 May 2020.
[47] 93 (2)
[48] S.107
[49] 93 (1)-(4).

3.2 ACCESS TO THE REGISTERS

Electoral registers, either in full or in part, are commonly made available to third parties, including both public and private entities. A general attitude towards openness and transparency in electoral matters has, for a long time, underpinned a widespread approach that voters' lists would be in the public domain and accessible to any interested person. However, in more recent times, growing concerns for voters' privacy and data protection have led in some cases to a change of culture, as illustrated below in the cases of Italy and Canada, for instance.

Nonetheless, it is still possible to observe instances of access to voters' lists granted on a widespread basis: for instance, in the UK, government departments and credit reference agencies are among the most common users of the full register, alongside political parties, campaigners, parliamentary and local government office holders, and candidates for election,[50] although the information contained in the register cannot be shared with any other person.[51] Copies of the open register can be purchased anyway from the registration officer by any person on payment of a fee,[52] and in fact are routinely acquired by businesses, charities, marketing firms and online directory firms.[53]

But most commonly access is granted specifically to individuals and organisations involved in electoral competitions: in France, candidates, political parties and other various groups[54] can obtain a copy of from local public offices under the condition of not making commercial use of it[55] and in Spain the register is available to candidates and their representatives.[56] The Italian case is

[50] r.103-104-105 RP(S)A; r.103-105 RP(NI)R; r.103-105 RP(W/E)R.
[51] r.101(6) RP(S)R; r.101(6) RP(NI)R; r.102(6) RP(E/W)R.
[52] r.109 RP(S)R; r.108 RP(NI)R; r.110 RP(E/W)R.
[53] ICO, *Electoral Register.*
[54] Electoral Code, Article L. 330-4.
[55] Instruction on the Keeping of Electoral Lists and Supplementary Electoral Lists
[56] Article 41(5)

exemplary of an approach becoming progressively more restrictive and yet still leaving ample leeway to political communication: whereas, in the late 1990s, the Italian Data Protection Authority had consistently maintained that electoral lists would be in the public domain and therefore accessible to any interested person irrespectively of their reason for accessing them,[57] successive legislative acts have progressively narrowed the range of legitimate purposes to access such information, until the current framework – largely devised to ensure compliance with the GDPR – limits access for 'purposes of electoral propaganda and relevant political communication' to personal data extracted from electoral registers held in municipal offices, provisional registers of Italian citizens resident abroad entitled to the right to vote including those voting abroad in EU Parliament elections and other similar lists.[58]

Outside Europe, the cases of Brazil and Canada offer two markedly different examples: in Brazil, political parties have full access to the information contained in the electoral register,[59] which is also made accessible to any public and private institutions and the general public, provided that basic principles of intimacy, private life, honour and personal image are respected.[60] In Canada, the law provides a relatively stricter framework, pursuant to which a registered party that endorsed a candidate in the electoral district in the last election can obtain a copy of the list of electors for the electoral district taken from the Register of Electors. Such lists, however, only include electors' names, addresses and unique identifiers.[61]

[57] Garante 22 luglio 1997, in Bollettino n. 1, pag. 43; 20 aprile 1998, in Bollettino n. 4, pag. 13.
[58] Provvedimento in materia di propaganda elettorale e comunicazione politica - 18 aprile 2019, para. 3 available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9105201
[59] Law 9.096 of 19 September 1995 Art 19§ (3)
[60] Resolution 21.538 of 14 October 2003 of the Superior Electoral Court Art 29.
[61] Elections Act (S.C. 2000, c. 9) S.45(2).

3.3 GROUNDS TO ACCESS THE REGISTERS

Different countries also take different approaches to the purposes for which access to electoral registers is granted. In some cases, it is possible to access information about voters for purposes largely irrelevant to political communications: in the UK, it is possible to buy copies of the full register and use the data for purposes including the administration of justice, enforcement of criminal law, vetting applications for credit, prevention of money laundering and statistical analysis of credit risk assessment.[62] Similarly, the open register can be sold for a wide range of purposes, including building (potential) customer databases in the private sector.[63]

By contrast, the approach taken by Spanish law seems particularly restrictive, as in fact it only allows access if requested through judicial channels.[64] In France, access to electors' lists can only be granted for non-commercial purposes;[65] this is assessed on the basis of a number of different indicators, such as the purpose of the intended activity, the legal status of the entity seeking to use the data, whether the of the re-user and whether or not the use is costly being mere indications in this respect; in any case, the circumstance where the data would be used to generate profit would be a decisive factor to consider the activity purely commercial.[66] The Italian law has progressively narrowed down the range of legitimate purposes to access electoral lists, once more in compliance with the GDPR: the long list of legitimate purposes including statistical, scientific or historical research, societal welfare and the generic 'common or public good'[67] provided for by a 2003 statute has now been abrogated, seemingly leaving only

[62] r.103-104-105 RP(S)A; r.103-105 RP(NI)R; r.103-105 RP(W/E)R
[63] ICO, *Electoral Register*
[64] Article 41(2)
[65] Instruction on the Keeping of Electoral Lists and Supplementary Electoral Lists
[66] Notice 20091074.
[67] D.lgs. 196/2003 Art 177

active and passive electoral rights as a legitimate reason to access electoral lists.[68]

In Canada, political parties and candidates can use electoral lists for communicating with electors, including using them for soliciting contributions and recruiting party members.[69] Any other use of the list is prohibited by the law[70] and constitutes and offence.[71] Much on a similar line, provincial laws forbid any further use other than communicating with electors, including for soliciting contributions and recruiting party members.[72] The provincial law of British Columbia allows the Chief electoral officer to include fictitious voter information so that unauthorised use can be traced.[73]

The analysis revealed a good degree of consistency across the board with respect to the kind of information included in the registers. More variety can be observed, instead, in how this information is made available to third parties. At one end of the spectrum, the UK is the case where voters' lists are widely accessible to different groups and in pursuit of different interests, whereas in other cases it is possible to observe a generalised trend towards limiting access to the registers. Barring access to commercial entities is now common practice, while political entities in different forms remain widely allowed to access the information contained in the lists, either in full or at least in part. The cases of France, where the law has devised a sort of dynamic test to assess the validity of the reasons for a request to access electors' lists and their commercial nature, and Canada, where the law provides a static definition of legitimate purposes to access the lists and makes an offence of the others, are examples of the possible different approaches that law-makers can resort to.

However, these measures are unfortunately far from enough – largely for two ranges of reasons. Firstly, it proves difficult to strike a suitable balance between competing interests: the growing awareness of the risks related with data

[68] Provvedimento in materia di propaganda elettorale e comunicazione politica - 18 aprile 2019, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9105201
[69] S.110.
[70] S. 111
[71] S. 487 (1) (b).
[72] Elections Act (Alberta) S20.
[73] Election Act (British Columbia) S. 51(3).

exploitation need to be balanced out against the principle of openness of the electoral process, and the legitimate interest of parties and campaigns to engage with voters in fulfilment of their own right to freedom of expression and the public's right to receive information relevant to the political debate.

On the other hand, the current dynamics of micro-targeting concern a much broader range of personal data than those traditionally considered as 'political' and granted enhanced protection. Other information revealing more general interests and behaviours are increasingly relied on in order to develop more individualised profiles.

4 COLLECTING DATA ON INDIVIDUALS' LIFESTYLE

By collecting data on individuals' lifestyle, campaigns are able to develop comprehensive behavioural tracking profiles of individual users, which in turn allows them to develop a range of different messages each tailored to appeal a different 'type' of voter. The UK's ICO has recognised that this is common practice for political parties and candidates, who normally use the register "as a 'spine' on which to add more granular and detailed information".[74] Permissive frameworks to access and collect lifestyle data about individuals are thus a major enabler for targeted digital messages.

According to the ICO, there are three methods by which personal data can be collected from third parties, some of which constitute a breach of the GDPR or domestic law. Firstly, buying or renting a list of contact details from third parties will be a breach of GDPR and possibly the Privacy and Electronic Communications Regulations unless the data subject has given explicit and specific consent. The practice of obtaining an individual's consent to use their data via a third party is only legitimate where the data subject had given their consent in a specific manner, rather than through a generic wording such as 'selected third parties', 'trusted partners' or 'for political campaigning purposes'.[75] Secondly, buying or renting factual personal data from a data broker or other third party is only permissible under condition that the data subject is given the appropriate information, including the buyer's privacy information.[76] Thirdly, the practice of buying or renting inferred personal data must comply with the GDPR when the nature of the data makes the data subject identifiable (otherwise, if the inferred data is anonymised it does not constitute personal data) and thus buyers are required to treat this data in the same way as factual personal data.[77] The UK's ICO guidance also establishes a

[74] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019, at pp.51-52
[75] ICO, Guidance on political campaigning: draft framework code for consultation, 2019, at p.58.
[76] *Ibid.*
[77] *Ibid.*, p.59.

duty of due diligence over data acquired from third parties, expecting parties to be able to demonstrate their compliance and be accountable.[78]

In principle, personal data from social media can be processed by political campaigners, however a key factor stressed by the ICO is that the public availability of information does not automatically deprive it of protection. GDPR and Privacy and Electronic Communications Regulations (PECR) safeguards still apply and, as a result, blanket collections of personal data from online sources including social media platforms are likely to constitute a breach of the data minimisation principle.[79] In fact, obtaining data in any of these ways automatically makes a party a data controller and as such expected to carry out a DPIA and mitigate against the risks.[80] In case a party or organisation runs a dedicated page on a social media platform, they qualify as a joint controller and therefore bear a joint responsibility for complying with data protection laws alongside the platform: they will need to provide appropriate privacy information to users and also ensure that the platform is also aware of the relevant obligations.[81]

The French data protection authority has released detailed guidance[82] for the use of data extracted from social networks. Inspired to a general principle of data minimisation, the guidance clarifies that making regular contact with a party or organisation through a specific channel (such as e-mails or a social network platforms) does not automatically imply a general consent to engage through other different means. Parties have limited options to harvest data from one channel and re-use it on a different one, depending on the level of pre-existing engagement with an individual: where a party was already in regular contact with a data subject through a channel, it would be allowed to reach out to them (for instance, by e-mail or private message) for the sole purpose of offering them regular electronic contact, although, should the person decline the

[78] *Ibid.*, p.59.
[79] *Ibid.*, 61-63.
[80] *Ibid.*
[81] *Ibid.*, p.61-62.
[82] Commission nationale de l'informatique et des libertés, 'Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?' [Political communication: what are the rules for using data from social networks?], 2016, https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

invite or not follow through, the party should have to delete the relevant information from their database. Occasional contacts (such as social media users who engaged occasionally with the party's profile, for instance by 'liking' it) but collecting any further data of theirs would be considered unfair. However, it would still be allowed to reach an occasional contact through the usual medium in order to obtain their consent to the collection of additional data concerning them. Other practices, such as collecting data from users with whom there has been no previous contact, or from social media's 'friends' lists' of users with whom the party has been in contact, either regularly or occasionally, are forbidden.

In Spain, personal data extracted from websites and other publicly accessible sources may be used for political purposes during electoral campaigns.[83] The electoral law only provides a fairly outdated framework leaving most current practices void of a solid legal basis, other than political surveys. However, more recent provisions seem to have introduced a less permissive regime: recent guidance from the data protection authority clarifies that such operations are only allowed during an electoral campaign (it is only possible to start making preparations, such as performing impact assessment or appoint a data protection officer) and at the end of the campaign the data must be deleted.[84] Organic Law 3/2018 has removed public interest as a permissible ground to process special category data and prohibits any processing of data for the main purpose of identifying a data subject's ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin even when the individual had consented to it.[85] In practice, Circular 1/2019 seems to have completely banned the most common practices leading to micro-targeting, making it difficult for political parties to collect information on people's lifestyle for political purposes. Article 7(4) of Circular 1/2019 establishes that the processing of any activity that may pose a risk to data subjects requires an impact assessment report and the advisory of the Spanish Data Protection

[83] LOREG Art 58 bis (2).
[84] Circular 1/2019 (entered into force on 11 March 2019) of the Spanish Data Protection Agency (Agencia Española para la Protección de Datos (AEPD)).
[85] Organic Law of Personal Data Protection and Digital Rights Guarantee 3/2018.

Agency to perform such activities, inserting a further hurdle for collecting lifestyle data about voters.

The Italian approach seems more detailed and partially more permissible. Consent to using personal data for political communications needs to be given specifically and separately from other purposes for which the data may be used, either in writing or on digital support. The current framework reveals an evident privileged position granted to political parties and any organisation pursuing political aims in general, as they are given more leeway to use data for communications purposes; however at the same time they also bear specific responsibilities in the process. The framework provides guidance about both the different categories of data that may be used for political communication, and the modes of collection that constitute a lawful basis for further processing.

With regard to the first issue, categories of data that may be used with the subject's consent include: data collected in a professional or business-related capacity, or for reasons connected to health care by medical personnel;[86] data included in telephone directories;[87] data collected from the Internet (such as telephone numbers or e-mail addresses), including when obtained by dedicated softwares (web or data scraping), or made available by the data subjects on their social media profiles.[88] Some other categories of data may be used by parties and political organisations without the subject's consent, such as personal data extracted from registers in the public domain (e.g. electoral registers held in municipal offices; additional lists of nationals of an EU member state resident in Italy who intend to exercise their right to vote in local elections)[89] and data of their own members and persons with whom they have regular contacts.[90] By contrast, personal data obtained by elected officials in the exercise of their functions cannot be used in any case.[91]

With regard to the second issue, the data subject's explicit consent and the clear identification of political communications as the purpose of data collection

[86] *Ibid.*, para. 5.C.
[87] *Ibid.*, para. 5.D.
[88] *Ibid.*, para. 5.E.
[89] *Ibid.*, para. 3.
[90] *Ibid.*, para 3.2.
[91] *Ibid.*, para. 5.B.

and processing are the standard legal basis. However, a certain degree of flexibility seems allowed: for instance, individuals who once consented to have their data collected on an occasion which implied their adherence to the organisation and their programme may find themselves contacted for further analogous initiatives, if the organisation's statute explicitly acknowledged this possibility at the time.[92] By contrast, if an association does not expressly pursue aims of political nature, then it may only use their members' personal data for political communications after obtaining explicit consent for this further aim.[93]

Political parties or individual candidates, when buying data from third parties, bear the duty to verify that the seller of the data had fulfilled all their legal obligations. Such a duty applies with regard to all the data subjects in case of databanks of modest dimensions (such as when they include a few hundreds or thousands of names) or, in case of larger databanks, to a sample objectively proportionate to the dimensions thereof, also having regard that the data collected is accurate and kept up to date.[94]

In Brazil, the General Data Protection Law requires that any processing of personal data (such as personal data on racial or ethnic origin, religious conviction, political opinion, trade union membership or religious, philosophical or political organisation, data concerning health or sex life, genetic or biometric data when linked to a data subject[95]) happens with the subject's specific consent,[96] and in compliance with principles such as clarity of purpose, adequacy of the processing techniques with the purpose pursued, data minimisation, data subject's right of access, accuracy, transparency, security, prevention of damage, non-discrimination and accountability.[97] Unlike the Spanish law that discards consent as a lawful ground for processing of special categories of data, the Brazilian LGPD allows consent as a lawful ground for processing special categories of data, which are called sensitive personal data.

[92] Provvedimento in materia di propaganda elettorale e comunicazione politica - 18 aprile 2019, para. 2.B, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9105201.
[93] *Ibid.*, para. 2.A.
[94] *Ibid.*, para 4.I.
[95] Art 5
[96] Article 11
[97] Article 6.

Canada is an example of an apparent legislative vacuum, as the Privacy Act regulates the collection of personal information by the federal government and the Personal Information Protection and Electronic Documents Act (PIPEDA) is only concerned with business and commercial activities;[98] as political parties fit neither of the two categories they are consequently not subject to federal privacy laws. They are instead subject to a special regime introduced through amendments to the Elections Act in December 2018, which requires political parties to submit and publish policies for protecting personal information.

The information presented by the parties ought to include: the types of personal information that the party collects and how it collects that information; how the party protects personal information under its control; how the party uses personal information under its control and under what circumstances that personal information may be sold to any person or entity; how the employees are trained; the party's practices concerning on-line privacy and use of cookies.[99] This provision has been criticised by the Chief electoral officer of Canada for its lack of minimum standards, oversight by an independent body, and mechanisms to allow Canadian citizens to validate or correct any information held by a party.[100]

British Columbia is the only province in Canada whose privacy laws cover political parties. As per guidance from the Privacy Commissioner of British Columbia[101] the Personal Information Protection Act (PIPA) governs the collection of personal information collected by political parties 'within British Columbia or about British Columbians'. The statute requires that any organisation acquires the subject's consent to collect, use or disseminate their data, after having

[98] Office of the Privacy Commissioner of Canada, 'Summary of Privacy Laws in Canada' (15 May 2014) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2> accessed 28 May 2020.
[99] Elections Act (S.C. 2000, c. 9) S. 385 (2)
[100] Democracy Under Threat: Risks And Solutions In The Era Of Disinformation And Data Monopoly Report of the Standing Committee on Access to Information, Privacy and Ethics' (House of Commons 2018) 22 <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.
[101] INVESTIGATION REPORT P19-01 Full Disclosure: Political Parties, Campaign Data, and Voter Consent' (Privacy Commissioner for British Columbia 2019) B.C.I.P.C.D. No. 07 5 <https://www.oipc.bc.ca/investigation-reports/2278> accessed 10 May 2020. https://www.oipc.bc.ca/investigation-reports/2278

communicated the purpose of the collection. It is possible in principle for an organisation to collect personal information from another without the consent of the individual, although the former must provide the latter with sufficient information regarding the purpose of the collection and allow it to determine whether the disclosure would be in accordance with the law.[102] Personal information about an individual may be acquired without consent or from a source other than the individual, if the information was already available to the public through directory assistance, a professional or business directory, a public registry or in a printed or electronic publication.[103]

As noted above, the collection of data on individuals' lifestyle is a relative novelty in the field of political communication, and it does not come as a surprise if most of the available regulation and guidance in this respect comes from data protection authorities' guidelines and other soft-law sources. In most cases, authorities such as the ICO in the UK, the CNIL in France, the Garante in Italy have demonstrated a good understanding of the most recent practices; the comprehensiveness of their guidance and the (relatively) swift time in which they were produced shows the increasingly central role played by data protection agencies (and comparable bodies) in this context. The practical measures introduced by the different authorities change even significantly from one case to another, although some trends can be observed across the countries considered in this study. The leeway granted to political organisations seems to be generally narrowing down, as authorities are now evidently paying attention and expect parties and campaigns to comply with more stringent procedures. There is an increasing emphasis on the transparency of data collection: the purpose of using data for political communications is now generally expected to be communicated explicitly, even in case the data is collected from third parties, and the subject's consent cannot be normally implied. Parties who acquire data for political communications are also generally expected to bear the responsibility to check that all prescribed procedures were respected. Nonetheless, practical provisions change significantly from one case to another. From a comparative perspective, a major divide can be noted

[102] S. 10 (1).
[103] S. 12 (1).

between those countries that exclude the possibility of processing some categories of data even with the subject's consent, and others that instead consider consent a lawful ground for processing any categories of data.

5 DATA CROSS-MATCHING AND PROFILING

Cross-matching and profiling allow campaigns to collate information gathered through different sources and, through sophisticated data analysis, develop (potentially) extremely precise assessments of individual preferences, interests and behaviour. From a technical standpoint, these practices are different than the mere collection of personal data as they refer, instead, to the subsequent processing thereof in order to extract relevant information about the data sabjects. Technological developments in the last few years have made possible to scale up the granularity of such operations, which now allow to target individual voters rather than just broader groups based on demographic similarities such as gender or age.

Data protection laws usually offer a degree of protection against abuses of such practices; however, while profiling is nowadays regularly used by marketers for commercial purposes, its use in the context of political campaigns proves more difficult to capture through general data protection laws as campaigns are often able to exploit gaps and loopholes, such as for instance the 'public task' basis for processing provided for in Art 6. For this reason, most recently regulators have begun to introduce bespoke provisions or guidance to specific address the issue and its specificities in the context of political communications.

The Commission guidance on the application of the GDPR suggests that political micro-targeting would meet the threshold for requiring consent under the GDPR when it has a 'legal or similarly significant effect on the individual',[104] emphasising the importance of the 'democratic vote' and the fact that 'it has the possible effect to stop individuals from voting or to make them vote in a specific way'.[105]

[104] Art.4(4), 22 GDPR.
'Commission Guidance on the Application of Union Data Protection Law in the Electoral Context' (European Commission 2018) 8 <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf>.

The guidance provided by the ICO in the UK allows any political party or candidate to carry out profiling for political campaigning purposes, provided that this is 'carried out fairly, transparently and in compliance with the law',[106] namely with requirements from the GDPR such as revising their privacy policy to inform individuals of the profiling being carried out, ensuring that collected personal data is kept accurate, and the amount of information collected and the length of time for which this will be kept is limited to the relevant purpose. The ICO also developed a list of questions designed to assess whether Art. 22 GDPR is engaged by profiling carried out in the course of political campaigning; if the profiling carried out in the course of political campaigning is restricted by Art. 22, the ICO stipulates that a series of requirements must be met, including for instance obtaining the data subject's explicit consent, and carrying out a DPIA.

Another example of DPA that has developed detailed guidance is Italy, where the Garante released a set of guidelines for on-line profiling.[107] These were, however, drafted in 2015, before the GDPR and the new Italian Data Protection Code were passed. The main underlying principles in the Guiding lines were those of informed consent and the principle that data collection should be related to the specific purpose sought. The articles in the old version of the Code to which the Guidelines made reference to have been formally abrogated, however the same principles are still part of the overall architecture of the GDPR. The Garante stressed that practices that consist of cross-matching users' data should only be allowed if compliant with data protection, on condition that the contracting party or user has given their consent after being informed in accordance with simplified arrangements, and thus recommended a series of measures to make consent notices easily accessible to all data subjects (e.g. via a single click from the website's landing page): any changes to the processing should be brought up to the data subjects in an easily understandable form, information to the data subjects should be organised on two levels so to make more immediately understandable, the same rules should apply to the same

[106] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019, at pp.68-69.
[107] Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line, 2015. Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3881513

types of processing irrespectively of the type of device which the data subject uses.

Compared to these two examples, France and Spain stand out for a notable lack of relevant provisions in their respective legal frameworks. In France, law 78-17 requires that any data cross-matching happens with the user's consent, as any legitimate interest of the data controller cannot prevail in lack of certain conditions, such as the subject's consent and a framework allowing them to object to such practices. In Spain, the law allows political parties to use personal data obtained from websites and other publicly accessible sources for the conduct of political activities during the electoral period.[108] However, when the main purpose of data processing amounts to identifying the data subject's sensitive information such as ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin, processing could be forbidden even in presence of the subject's consent.[109]

In Canada such profiling would also likely require express consent.[110] Moreover, the use of profiling to infer information about a voter such as their ethnicity and gender (these predictions are treated as 'creating new information about a person') is equally likely to require consent because this usage goes beyond the reasonable expectations of the data subject. Moreover, such predictive profiling may lead to the collection of inaccurate data which is equally contrary to the law.[111]

In Brazil, the processing of sensitive personal data such as that used in profiling likely requires express consent[112] and the data subject has a right to "request a review of decisions taken solely on the basis of automated processing of

[108] LOREG Art 58bis.
[109] LOPDGDD Art 9.
[110] 'INVESTIGATION REPORT P19-01 Full Disclosure: Political Parties, Campaign Data, and Voter Consent' (Privacy Commissioner for British Columbia 2019) 23 <https://www.oipc.bc.ca/investigation-reports/2278> accessed 10 May 2020; Office of the Privacy Commissioner of Canada, 'PIPEDA Report of Findings #2019-004: Joint Investigation of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia' (26 November 2019) <https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/?wbdisable=true> accessed 29 May 2020.
[111] 'INVESTIGATION REPORT P19-01 Full Disclosure: Political Parties, Campaign Data, and Voter Consent' (Privacy Commissioner for British Columbia 2019) 22.
[112] Article 11 LGPD

personal data affecting his interests, including decisions aimed at defining his personal, professional, consumer and credit profile or personality aspects." [113]

At this stage of the process, the countries considered show a significant degree of diversification in their respective approaches. Most notably, significant differences exist between countries whose data protection authorities have provided relevant guidance, in a more or less detailed form, and others where the relevant framework is largely silent on the issue. Other differences emerge in the role played by the data subject's consent, in some cases a sufficient legal basis for cross-matching but not in all the countries examined, and the need for detailed guidance as to the different aims and circumstances that lead to situations where cross-matching would not be allowed or the controller would need to comply with further requirements – a profile in which respect several of the frameworks examined seem to lack of clarity at present.

[113] Article 20 LGPD

6 PERSONALISED COMMUNICATIONS

Where personal data has been collected from an individual and subjected to data cross-matching or profiling, the third step consists of using this information to send personalised communications to the data subject. The process is known broadly as 'direct marketing'.[114] It is becoming increasingly frequently used by political campaigns to promote candidates and influence potential voters.[115]

This last step in the process of transmitting micro-targeted communications is most commonly addressed in the context of regulatory frameworks for political communications. Every jurisdiction examined in this comparative analysis has adopted legislative provisions to improve the transparency of digital political campaigning in some form. However, these approaches differ significantly and have had varying success.

A particularly strong example is the provision in Spain which specifies that all electoral propaganda distributed by electronic messaging or social media networks "must state their electoral nature and the identity of the sender".[116] Similarly in Brazil, a clear labelling requirement has been established as follows:

> *'It is forbidden to broadcast any type of paid electoral propaganda on the Internet, except for the boost content, provided that it is unequivocally identified as such and contracted exclusively by political parties, coalitions and candidates and their representatives.'*[117]

In France, online platform operators are under a clear obligation to

> *'…provide the user with fair, clear and transparent information on the identity of the person, the name, the registered office and corporate purpose of the legal entity and that of the legal entity for which it is*

[114] For UK definition of "direct marketing" see Data Protection Act 2018 s.122(5)
[115] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019 at p.74
[116] Circular 1/2019 Article 11(3)
[117] Resolution 23.610 of 18 December 2019 Article 29

> *established, the account of which, where applicable, it has declared that it is acting, which pays to the platform remuneration in counterpart of the promotion of information content related to a debate of general interest.*[118]

While the nature of the information that must be provided by platform operators has been explained in detail, a criticism of the French provision is that it applies only for the three months preceding the first day of the general election month until the date when the candidate is elected.[119]

In the UK printed election publications must clearly identify the printer and promoter of the material,[120] however this information is not yet obligatory for political direct marketing conducted digitally.[121] The UK is subject to the Privacy and Electronic Communications (EC Directive) Regulations 2003 which stipulate that electronic mail may only be used for direct marketing purposes providing that the sender does not conceal their identity.[122] However, according to the Information Commissioner's Office, "electronic mail does not include advertising through social media and other online platforms, even where directed at particular individual".[123]

The Electoral Commission, Electoral Reform Society and Law Commissions have all voiced their support for the introduction of an "imprint requirement" in the UK that would compel online campaign material to show where the ad has come from and how it has been funded.[124] This has already been agreed to by the Government which made a commitment in May 2019 to implement an imprints regime for election campaign material online.[125] It is also worth noting that an imprint requirement for online election material has recently been extended to all referendums held in Scotland by the Referendums (Scotland) Act 2020.[126]

---

[118] Article L163-1
[119] Article L163-1
[120] Representation of the People Act 1983 s.110 and Political Parties, Elections and Referendums Act 2000
[121] Law Commission and Scottish Law Commission, *Electoral Law: A joint final report*, law Com No. 389, Scot Law Com No 256, 16 March 2020, at p.157 para. 12.40
[122] Privacy and Electronic Communications (EC Directive) Regulations 2003 Reg 22 and 23
[123] ICO, *Guidance on political campaigning: draft framework code for consultation*, 2019, at p.79
[124] Law Commission and Scottish Law Commission, *Electoral Law: A joint final report*, Law Com No.389, Scot Law Com No 256, 16 March 2020, recommendation 77 at p.201 para 15.77
[125] UK Government, *Government safeguards UK elections*, 5 May 2019, available at: https://www.gov.uk/government/news/government-safeguards-uk-elections
[126] Referendums (Scotland) Act 2020 s.13 and Sch.3 para 28(1)(b) and (9)

In Italy, the Media Authority has introduced guidelines on the equality of access to online platforms which stress that the existing regulatory framework for the print and broadcast sector should apply as far as possible to online platforms also.[127] These guidelines specifically state that:

> '*[a]dvertisers should clearly label political ads as such and identify their source, similarly to the requirements already in place for the print and broadcasting sectors."*[128]

While the use of imprint requirements is one way to improve the transparency of personalised communications and direct marketing, another possibility for reform is creating a single, publicly available and searchable, online database of political adverts.[129] This approach was adopted in Canada with the creation of the "Registry of Partisan Advertising Messages and Election Advertising Messages". The statutory basis for this Registry establishes that:

> *'[t]he owner or operator of an online platform that sells, directly or indirectly, advertising space to the following persons and groups shall publish on the platform a registry of the persons' and groups' partisan advertising messages and election advertising messages published on the platform during that period."*[130]

Although each legal jurisdiction subject to analysis has taken a different approach to improving the transparency of political direct marketing online, it is clear that such personalised communications must be suitably transparent for recipients to fully understand their nature and origin.

The most common means of ensuring such transparency is through the introduction of an 'imprint requirement' for online political ads. However, such a

[127] Autorità per le Garanzie nelle Comunicazioni, Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018. Available at: https://www.agcom.it/documents/10179/9478149/Documento+generico+01-02-2018/45429524-3f31-4195-bf46-4f2863af0ff6?version=1.0

[128] Autorità per le Garanzie nelle Comunicazioni, Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018 para.2

[129] Electoral Reform Society, *Reigning in the Political Wild West: Campaign Rules for the 21st Century*, February 2019 at p.13; see also Electoral Commission, Digital Campaigning – increasing transparency for voters, 13 August 2019, available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters

[130] Elections Act (S.C. 2000, c.9) s.325.1(2)

requirement must be properly drafted and cover election material at all times, not only during a specific campaigning period.

An alternative method which has been used successfully in Canada is the introduction of a database where members of the public can readily access information on any online advertising messages. This has great potential to improve the transparency of digital campaigning as a whole and there is legitimate scope for such a provision to be implemented in other jurisdictions, including the UK. In fact, this provision recalls closely the measure introduced, in the EU, with the Code of Practice on disinformation which now incentivises platforms to maintain repositories of political ads, although in the first annual self-assessment of the signatories released in late 2019 the Commission noted that the data available in these repositories was still limited, particularly in regard to the targeting criteria used by political advertisers.[131]

[131] EU Commission, 'Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019', at https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

7 CONCLUDING REMARKS

The analysis has revealed a number of common trends and some striking differences across the six countries examined.

None of those provides a comprehensive, unitary framework for micro-targeted political communications, and all resort instead to piecemeal approaches where the potential for gaps and loopholes is all too often exploited by campaigns. Against this background, Data Protection Authorities are often emerging as the regulators with the most systematic approach to tackle this challenge. A common finding from the comparative analysis is the general difficulty to bar access to personal data. The amount of data available in the public domain, and legitimate interests in making data available for promoting democratic engagement and similar aims often frustrate efforts to cut micro-targeting practices off at their origin. However, new emerging trends such as barring commercial entities from accessing electoral registers, a generalised increasing emphasis on the transparency of data collection, and expecting parties and campaigns to bear a responsibility for the legitimacy of their data processing practices are clear signs of a widespread growing awareness of the inherent risks of such form of communication. Conversely, the requirement of the consent of data subjects is in some cases now accompanied with further requirements, which in all likeliness is a sign of the rising recognition of the unsuitability of this sole condition to govern this field.

With regard to personalised communications, each legal jurisdiction has taken a different approach to improving the transparency of political direct marketing online; despite the lack of consistency at the comparative level, transparency is evidently emerging as a key requisite to expect campaigns and other entities involved in such practices, either (as most commonly required at present) through the introduction of an 'imprint requirement' for online political ads, or other equivalent means.

Comparative analysis suggests that, in light of current trends and technological developments, the most effective means of challenging exploitative digital

political campaigning in the context of direct marketing is to improve the transparency of online communications. However, emerging trends in regard to data collection and matching practices highlight the urgency of devising consistent and comprehensive legal frameworks to ensure that adequate safeguards are present throughout the production chain of targeted political communications.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

privacyinternational.org

School of Law, University of Edinburgh
Old College, South Bridge
Edinburgh EH8 9YL
United Kingdom

law.ed.ac.uk